Hakin9

HARD CORE IT SECURITY MAGAZINE

Hakin9 Ausgabe 5/2011 Mai Monats- Online-Magazin

PHISHING

MIT SOZIALEN NETZWERKEN

PSW GROUP

SSL-Zertifikate

Einkaufen ist Vertrauenssache - online und offline!

Vertrauen Sie auf über **10 Jahre** Erfahrung

UNSERE PRODUKTE

- Domain Validation (DV)-Zertifikate
- Organization Validation (OV)-Zertifikate
- Extended Validation (EV)-Zertifikate

- Single-Zertifikate
- Wildcard-Zertifikate
- Multidomain (MDC)-Zertifikate
- Unified Communication / Subject Alternative Name (UCC/SAN)-Zertifikate
- Server Gated Cryptographie (SGC)-Zertifikate

Ihre Vorteile

Bis zu **90 Tage** längere Laufzeit*

Jederzeit **kostenloser Austausch**

Zusätzliche Lizenzen **ohne Aufpreis***

Unkomplizierte Lieferung **auf Rechnung****

Persönlicher Support
in deutsch, englisch, spanisch und polnisch

* in den Produktlinien Lite, Silver und Gold

** bei Pay-as-you-Go

VeriSign · GeoTrust · thawte · COMODO Creating Trust Online · GlobalSign

LIEBE HAKIN9 LESER!

Das Hauptthema dieser Ausgabe ist *Phishing mit sozialen* Netzwerken. In dem Artikel wird beschreibt, wie auf Grund der Verbreitung von sozialen Netzwerken persönliche Informationen für neuartige Social Engineering Angriffe missbraucht werden können. Der Artikel finden Sie im Bereich *Technik*, auf der Seite 7.

In der Rubrik *Sicherheit* stellen wir Ihnen auch Kleinste Programmierfehler, ein falsches Wort in der Google Adwords Kampagne oder die nicht erlaubte Verwendung von Bild- und Tonelementen auf der Website dar. Dieser Artikel lesen Sie auf der Seite 13.

Wir möchten Ihnen auch im Artikel *Netzwerk-Sicherheit – Schutz eines Netzwerks durch ein Check Point Security Gateway*, eine sehr flexible Security Architektur für Unternehmen präsentiesen. Der Artikel von Stefan Schurtz finden Sie auf der Seite 20.

Ich hoffe, dass wir mit dieser Ausgabe Ihren Herausforderungen gewachsen sind.

Wenn Sie Ideen, Bemerkungen oder Tipps für Hakin9 haben, nehmen Sie sich kurz Zeit und beantworten die 11 Fragen, die unter: *http://hakin9.org/de/leserumfrage* zu finden sind. Ihre Meinung ist uns wichtig. Damit helfen Sie uns das hakin9 IT Security Magazin noch besser zu gestalten und weiterzuentwickeln.

Viel Spaß bei der Lektüre!
Karolina Sokołowska

hakin9

hakin9

5/2011

INHALTSVERZEICHNIS

TECHNIK

SICHERHEIT

INFORMATIONS-SICHERHEIT

ABWEHR

EXPERTENBEREICH PSW GROUP

hakin9

herausgegeben vom Verlag:
Software Press Sp. z o. o. SK

Geschäftsführer: Paweł Marciniak

Managing Director: Justyna Książek
justyna.ksiazek@software.com.pl

Chefredakteurin: Karolina Sokołowska
karolina.sokolowska@software.com.pl
Redaktionsassistentin: Ilona Przybysławska
Ilona.przybyslawska@software.com.pl

Redaktion: Markus Huber, Peter Kieseberg, Matthias Talpa, Willem Vooijs, Stefan Schurtz, Christian Heutger, Erich Scheiber, Peter Soudat, Gustav Jung, Herfried Geyer, Johannes Mariel, Karin Peyerl, Kilian Zantop, Robert Lommen, Michael Schratt, Thomas Hackner

Produktion: Andrzej Kuca

DTP: Przemysław Banasiewicz

Umschlagsentwurf: Przemysław Banasiewicz

Werbung: adv@software.com.pl

Anschrift:
Software Press Sp. z o.o. SK
ul. Bokserska 1, 02-682 Warszawa, Poland
Tel. +48 22 427 36 56, Fax +48 22 244 24 59
www.hakin9.org/de

hakin9 erscheint in folgenden Sprachversionen und Ländern: deutsche Version (Deutschland, Schweiz, Österreich, Luxemburg), französische Version (Frankreich, Kanada, Belgien, Marokko), spanische Version (Spanien, Portugal), polnische Version (Polen), englische Version (Kanada, USA)

EXPERTENBEREICH CIS

DATENSICHERHEIT

Im Zusammenhang mit den Änderungen, die in letzter Zeit in dem deutschen Recht stattgefunden haben und die IT-Sicherheit betreffen, möchten wir ankündigen, dass hakin9-Abwehrmethoden Magazin seinem Profil treu bleibt.

Unser Magazin dient ausschließlich den Erkenntniszwecken. Alle im Magazin präsentierten Methoden sollen für eine sichere IT fungieren. Wir legen einen großen Wert auf die Entwicklung von einem sicheren elektronischen Umsatz im Internet und der Bekämpfung von IT Kriminalität.

Bachelor-Studiengang IT Security
Master-Studiengang Information Security

IT-Infrastruktur sichern und managen.

Das Studium vermittelt eine integrale, ganzheitliche Sicht der Security von IT-Infrastruktur. Die Kombination aus Technik- und Managementwissen ist in Österreich einzigartig. Sie bildet die Grundlage für die zukünftigen Security-ExpertInnen im Unternehmen, die sowohl die technischen Kenntnisse für einen sicheren IT-Betrieb beherrschen als auch mit Management-Aufgaben vertraut sind.

Immer mehr Prozesse eines Unternehmens werden EDV-unterstützt abgebildet und abgewickelt. Computerviren, Hacker, Datenverluste, Webattacken usw. stellen somit eine Bedrohung für die IT-Infrastruktur eines Unternehmens dar. Immer wieder hört man, dass hochsensible Daten verloren gehen oder in falsche Hände geraten. Bei einem Ausfall der IT-Infrastruktur können wichtige Tätigkeiten nicht mehr erledigt werden, was zu einem beträchtlichen finanziellen Schaden für das Unternehmen führen kann. Daraus resultierend ergibt sich eine große Nachfrage an Security-ExpertInnen, die sowohl die technischen Kenntnisse für einen sicheren IT-Betrieb aufweisen, als auch mit Management-Aufgaben vertraut sind.

Ausbildungschwerpunkte:

- IT-Betrieb
- Netzwerktechnik
- Sicherheitstechnologien
- Sicherheitsmanagement und Organisation

Wählen Sie ab dem 3. Semester folgende individuelle Schwerpunkte: Forensik, Fraud Investigation, Botnet Detection und Malware.

Der **Master-Studiengang Information Security** ist als konsekutiver Studiengang auf dem **Bachelor-Studiengang IT Security** aufgebaut.
Im Masterstudiengang wird der Kompetenzerwerb durch fächerübergreifende Problemstellungen, Forschungsseminare, Projekte und der wissenschaftlichen Abschlussarbeit (Diplomarbeit) sichergestellt. Diese **2-stufige Ausbildung** macht die AbsolventInnen zu gefragten ExpertInnen.

Berufsfelder:

- Sicherheitsbeauftragte/r (Chief Information-Security-Officer)
- Compliance Officer, Risikomanager
- IT-Governance ExpertIn
- Datenschutzbeauftragte/r
- AuditorIn
- IT Security Solution Engineer/Architect
- Security-Consultant
- IT Infrastructure Engineer
- Security Quality Assurance ManagerIn
- Software Architect
- IT-Solution Architect

Die AbsolventInnen sind qualifiziert, leitende und planende Tätigkeiten auszuführen.

Zertifizierungen

Im Rahmen des Studiums können folgende Zertifizierungen erworben werden:

- **CCNA** – CISCO Certified Network Associate
- **CCNP** – CISCO Career Certifications & Paths
- **PHSE** – PHION Security Engineer
- **MCITP** – Microsoft Certified IT Professional
- **ITIL V3**

Get certified and you're on the spot!

Mit dieser Kombination aus Technik- und Managementwissen zum/zur gesuchten SicherheitsexpertIn!

Jetzt bewerben!

Aufnahmetermine:
2. + 26. April und 7. Juni 2011
Bewerbungsfrist: 24. Mai 2011

Fachhochschule St. Pölten GmbH
Matthias Corvinus-Straße 15
3100 St. Pölten, Austria
T: +43/2742/313 228 - 632
E: is@fhstp.ac.at, I: www.fhstp.ac.at

Phishing mit sozialen Netzwerken

Markus Huber und Peter Kieseberg

In diesem Artikel beschreiben wir, wie auf Grund der Verbreitung von sozialen Netzwerken persönliche Informationen für neuartige Social Engineering Angriffe missbraucht werden können.

IN DIESEM ARTIKEL ERFAHREN SIE...

- Die Auswirkungen von sozialen Netzwerken auf Spam und Phishing-Attacken
- Beschreibung des Friend-in-the-middle-Angriffs

WAS SIE VORHER WISSEN SOLLTEN...

- Grundlegende Computerkenntnisse
- Grundlegende Kenntnis von sozialen Netzwerken

Social Engineering

Social Engineering ist die Kunst das schwächste Glied eines gesicherten IT-Systems auszunutzen: Den Benutzer. Im Unterschied zu technischen Angriffen werden dabei Mittel der Beeinflussung eingesetzt um an Informationen zu gelangen, oder Personen anderweitig zu manipulieren. Prinzipiell handelt es sich dabei um keine gänzlich neue Angriffsform, allerdings wurde diese erst im Zuge der Aktionen von Kevin Mitnick Ende der 80-er / Anfang der 90-er Jahre einer breiteren Öffentlichkeit bekannt. Ausgangspunkt bei diesen Angriffen war oftmals das sogenannte „dumpster diving“ - die Müllkübel großer Firmen und anderer Organisationen wurden auf der Suche nach verwertbarem Material (Telefonlisten, Personalverzeichnisse, vertrauliche interne Informationen) durchsucht. Diese Daten verwendete man in weiterer Folge als Grundlage für gezielte Angriffe auf Mitarbeiter (bspw. Aushorchen in persönlichen Gesprächen, Manipulation von Mitarbeitern durch Täuschung oder Aufbau von Druck).

Schon zu dieser Zeit galt Social Engineering als sehr erfolgversprechend und schwierig zu verhindern, jedoch ebenfalls als relativ teuer (hoher Zeitaufwand in der Vorbereitung und Durchführung).

Social Engineering in Web2.0

Mit der steigenden Popularität von sozialen Netzwerken wie bspw. Facebook, geben immer mehr Personen persönliche Informationen über sich selbst, aber auch über „Freunde“ preis. Angreifer können also viele der Informationen, für die früher dumpster diving betrieben werden musste, komfortabel im Netz recherchieren. Außerdem liegt nun die Information unmittelbar in maschinell und automatisiert weiterverarbeitbarer Form vor, sodass Social Engineering großteils durch Tools eigenständig betrieben werden kann. Im Gegensatz zur Ära des dumpster diving ist Social Engineering damit bedeutend günstiger in der Durchführung.

Social Phishing und Social Spam

Klassisches Phishing und speziell Spaming stellen Streuangriffe dar, bei denen große Benutzermengen mit der gleichen Nachricht bombardiert werden und darauf gehofft wird, dass mit dem relativ kleinen Anteil an Empfängern, die darauf tatsächlich reagieren letztendlich Gewinn gemacht wird. Prinzipiell gilt der Anteil der Personen, die auf diese Art von Nachrichten reagieren als relativ gering. Die Zieladressen werden zumeist mit Hilfe von Webcrawlern oder durch trial-and-error (raten) eruiert, daher sind viele dieser Adressen ungültig und damit wertlos.

Spear-Phishing und Pharming bzw. das Whaling sind als Spezialfälle des klassischen Phishings anzusehen. Beim Spear-Phishing wird auf eine eingeschränkte, homogen(er)e Gruppe (bspw. Studenten einer speziellen Universität) abgezielt, dadurch können die elektronischen Nachrichten viel spezieller auf Bedürfnisse und (vermutete) Interessen eingehen. Ist der gezielte An-

griff gegen hohe Führungskräfte gerichtet, dann spricht man auch oft vom sogenannten Whaling. Pharming hingegen ist eine technische Weiterentwicklung des Phishings, bei dem durch Manipulation des DNS-Lookups trotz Eingabe der richtigen Webadresse gefälschte Webseiten angezeigt werden können.

Im Gegensatz zur klassischen Vorgangsweise sind die Web2.0-Varianten dieser klassischen Angriffe wesentlich fokussierter und auf eine Zielgruppe bzw. sogar auf individuelle Ziele zugeschnitten. Viele soziale Netzwerke stellen persönliche Informationen ihrer Nutzer bereit (Namen, Interessen, Geburtstag, …). Die Angreifer verwenden diese Daten um ihre Angriffe glaubhafter zu machen. Die Phishing-Mails werden mit Hilfe von Tools automatisch aus Templates erstellt und mit den gewonnenen persönlichen Informationen angereichert. Ein Beispiel für so ein Tool ist die im „Social Engineer Toolkit" enthaltene Mailingfunktionalität. Im Prinzip wird beim Social Phishing die Vertrauensstellung zwischen „befreundeten" Usern ausgenützt. Dabei kann das soziale Netzwerk selbst für das Senden von Spam verwendet werden, zum Beispiel über Einträge in der Benutzer-Pinnwand (Wall) oder durch private Nachrichten.

Social Spam zeichnet sich dadurch aus, dass auf Basis von gesammelten Daten persönliche Informationen in die Gestaltung der Spammails fließen. Abbildung 1 stellt die unterschiedlichen Ansätze gegenüber: Verwendung der korrekten Sprache, des richtigen Namens und das Ausnutzen einer bestehenden Freundschaftsbeziehung zur Vortäuschung der Empfehlung.

In weiterer Folge wollen wir ein kombiniertes Bedrohungsszenario bestehend aus Social Phishing und Social Spam vorstellen – die Friend-in-the-middle Attacke:

Social Engineering

Social Engineering ist die Kunst das schwächste Glied eines gesicherten IT-Systems auszunutzen: Den Benutzer.

Phishing

Phishing ist ein Kunstwort, das sich an die Wörter „password" und „fishing" anlehnt. Gemeint ist damit das Herauslocken von Zugangsdaten (Username und Passwort). Dabei geben sich die „Phisher" als vertrauenswürdige Personen oder Institutionen aus und versuchen mit gefälschten elektronischen Nachrichten an Zugangsdaten zu gelangen.

Friend-in-the-middle (FiTM)

Wir definieren Friend-in-the-Middle-Angriffe als aktive Lauschangriffe gegen soziale Netzwerk Services. Unser FiTM Angriff basiert auf dem fehlenden Schutz der Kommunikationsverbindung zwischen Benutzer und sozialen Netzwerk Services. Durch das „hijacking" von Session-Cookies wird es möglich, eine Interaktion mit dem sozialen Netzwerk ohne entsprechende Genehmigung des entführten Benutzerkontoinhabers durchzuführen. Cookie-session hijacking ist ein altbekannter

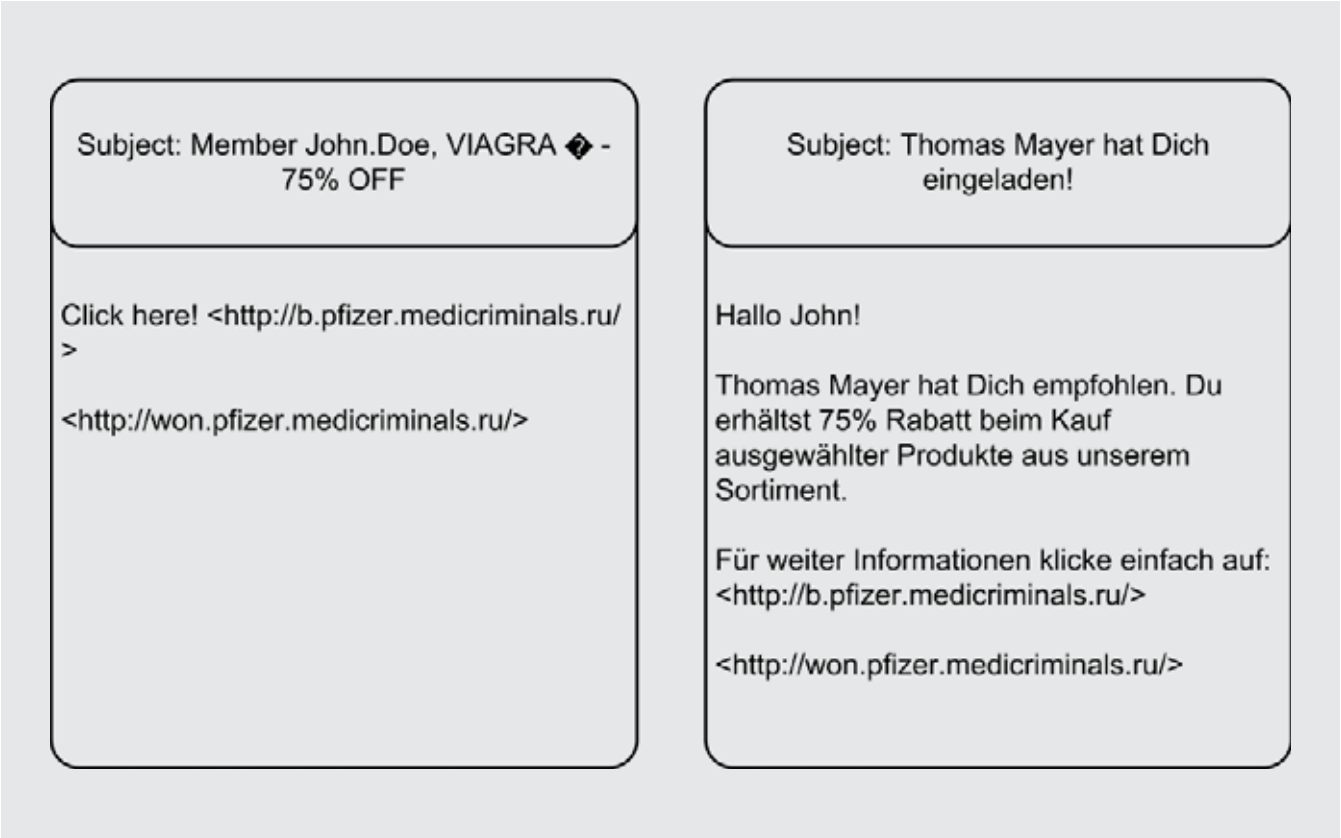


Abbildung 1. *Klassischer Spam versus Social Spam*

Angriff gegen Web-Services. Im Zusammenhang mit den neuartigen sozialen Netzwerken führt dieser Angriff jedoch zu einer Reihe von weiterführenden, komplexeren Angriffsszenarien. Mit der Ausnahme von XING bieten die meisten sozialen Netzwerke keine standardmäßige Vollverschlüsselung (HTTPS) der zwischen den Benutzer und Servern übertragenden Informationen. Da soziale Netzwerke aufgrund ihrer Popularität bereits für einen gehörigen Anteil des weltweiten www-Traffics verantwortlich sind, können ungeschützte soziale Netzwerksitzungen quasi überall (bspw. WLAN, Firmennetzwerk) unverschlüsselt beobachtet werden.

Entführte Benutzersitzungen können in der Folge für friend injection, application injection, sowie Social Engineering missbraucht werden. Bei friend injections fügt der Angreifer sich als Freund des angegriffenen Benutzerkontos hinzu um somit dessen geschlossenes Netzwerk zu infiltrieren. Neben Freunden lassen sich auch bösartige Anwendungen zum Benutzerkonto hinzufügen (Application injection). Eine Anwendung die unter der Kontrolle des Angreifers ist, kann benutzt werden um die Daten des Benutzerkontos zu extrahieren. Zuletzt ermöglichen entführte Verbindungen, wie im vorangegangenen Abschnitt beschrieben, gezielte Social Engineering Angriffe auf Benutzer und deren Freunde.

Social Spam Angriffe mittels FiTM

Es gibt verschiedene Ansätze um Spam-und Phishing-Nachrichten mittels FiTM-Angriffen zu versenden. Das soziale Netzwerk selbst könnte für das Senden von Spam verwendet werden, zum Beispiel über Einträge in der Benutzer-Pinnwand (Wall) oder durch private Nachrichten.

Wenn diese internen Kommunikationsmöglichkeiten allerdings in großem Umfang missbraucht werden, ist es wahrscheinlich dass ein solcher Angriff von den sozialen Netzwerk -Serviceprovidern erkannt wird, da diese bereits eine Reihe von Anti-Spam-Strategien zum Schutz ihrer Netzwerke implementiert haben. Ein vielversprechender Ansatz (aus Sicht des Angreifers) ist das Versenden von „out-of-bound“-Spam-Nachrichten. Out-of-bound-Nachricht bedeutet, dass traditionelle E-Mails oder andere Formen für das Senden von Spam- und Phishing-Nachrichten benutzt werden. Dieser E-Mail-Spam wird durch die Verfügbarkeit von echten E-Mail-Adressen ermöglicht, die von den Benutzern im

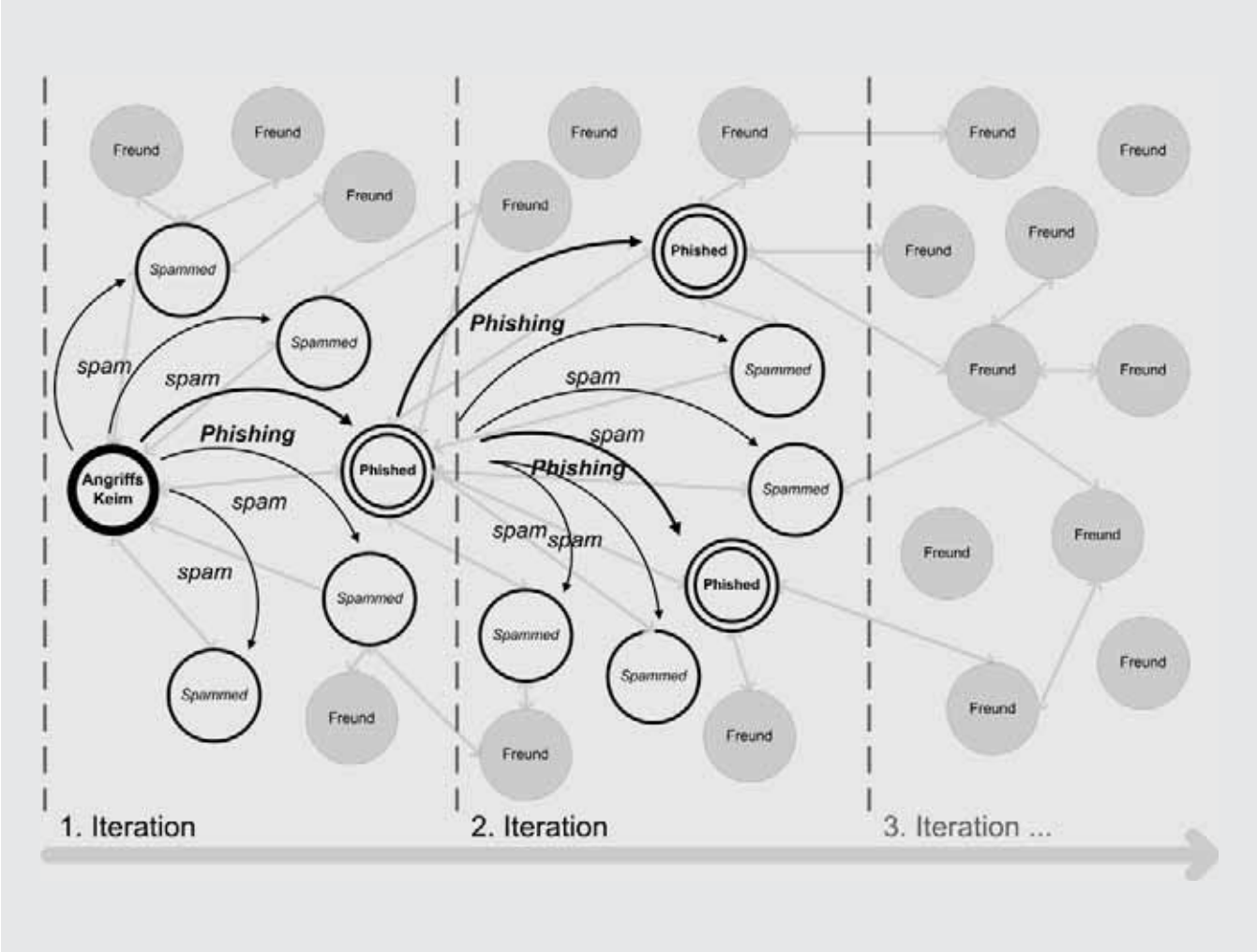


Abbildung 2. *Friend-in-the-middle-Angriff*

Rahmen des sozialen Netzwerks veröffentlicht werden. Wenn also die Spam-Attacke über E-Mail anstelle innerhalb der Plattformen durchgeführt wird, können diese Nachrichten nicht von den sozialen Netzwerk-Serviceprovidern erfasst werden. In der Folge beschreiben wir einen großflächigen Spam-Angriff auf Basis von FiTM. In unserem Szenario werden soziale Netzwerksitzungen vorübergehend übernommen und dienen als „Angriffskeime". Informationen die über diese Keime gesammelt werden, werden dann verwendet, um sowohl sozialen Spam, als auch soziale Phishing-Mails zu generieren. Der Angreifer tarnt sich hierbei mit Hilfe von extrahierten Bilder und persönlichen Informationen als ein Freund des Spam-Opfers und wird so zum „Friend-In-The-Middle".

- Abbildung 2 zeigt den Überblick einer Spam-Kampagne auf Basis unserer FiTM Angriffe. Im ersten Schritt wird eine Netzwerkverbindung überwacht. Sobald die FiTM-Anwendung eine aktive Social-Networking-Session erkennt, klont es den kompletten HTTP-Header inklusive der Session-Cookies.
- Der geklonte HTTP-Header dient nun als Authentisierungsschlüssel für ein bestimmtes soziales Netzwerk und wird verwendet, um Benutzersitzungen vorübergehend zu übernehmen.
- Um die Profilinhalte sowie Informationen über die Ziel-Freunde zu extrahieren, wird eine spezielle Drittanwendung zum angegriffenen Profil hinzugefügt. Sobald alle Informationen gewonnen wurden, wird die Anwendung aus dem Profil entfernt. Zusätzliche Abfragen werden verwendet, um die Emailadressen aller Freunde des Zielprofiles zu sammeln, falls sie nicht durch eine selbstgeschriebene Anwendung abgerufen werden können.
- Die extrahierten Emailadressen und Profilinhalte werden dann verwendet, um maßgeschneiderte Spam- und Phishing-E-Mails zu generieren. Während die Spam-Nachrichten die eigentliche „payload" des Angriffs darstellt, werden die Phishing-Mails verwendet um die Anmeldeinformationen weiterer Benutzerkonten für die Vermehrung zu stehlen (die FiTM Angriff beginnt wieder aus (3) mit den gephishten Anmeldeinformationen als Ausgangspunkt).

Simulation von FiTM – der Facebook-Fall

Um Aussagen über die Auswirkungen eines FiTM Spam Angriffes zu treffen, entschieden wir uns für ein Experiment auf Basis von Facebook. Zu einem Teil war es unser Ziel herauszufinden wie viele mögliche Facebook-Sessions wir übernehmen könnten und zum anderen zu simulieren, wie hoch die Anzahl der gesamten Spamziele wäre. FiTM Angriffe auf Facebook-Basis dienen unserer Meinung nach als gutes Beispiel, da es zu dieser Zeit bei weitem das größte soziale Netzwerk ist, HTTPS standardmäßig nur verwendet wird um Zugangsdaten zu schützen und Facebook Drittanwendungen unterstützt. Darüber hinaus verspricht die Injection von Drittanbieter-Anwendungen in Facebook-Profile Zugang zu einer Fülle von persönlichen Informationen.

Zur Durchführung der FiTM Angriffe können zahlreiche Angriffsmethoden verwendet werden: DNS-Poisoning, Cross-Site Request Forgery, unverschlüsselte drahtlose Netzwerke, Deep Packet Inspection von einem ISP oder anderen bösartigen Dritten, die Zugriff auf den Datenverkehr zwischen dem Benutzer und dem sozialen Netzwerk haben. Allerdings haben wir unsere Proof-of-Concept-FiTM Anwendung zur Analyse von Facebook HTTP-Cookies, die ein Tor-Exit-Node durchlaufen, verwendet. Das Tor-Netzwerk ist ein weit verbreitetes Anonymisierungs-Netzwerk, das Nutzer-IP-Adressen im Internet verschleiert. Es wird angenommen, dass dieses Netzwerk von hunderttausenden Anwendern täglich genutzt wird und es gilt als eines der am stärksten verbreiteten Anonymisierungs-Netzwerke. Die Tor-Infrastruktur basiert auf Servern die von Freiwilligen betrieben werden, daher kann jeder das Tor-Projekt durch die Einrichtung eines dedizierten Tor-Servers unterstützen. Für unser Experiment haben wir ein Tor-Exit-Node auf einen minimalen GNU / Linux Debian-Server mit einer Bandbreite von 5 Mbit aufgesetzt. Der Server wurde zudem so konfiguriert, dass HTTP-Datenverkehr (TCP Port 80) aus dem Tor-Netzwerk mit dem Internet erlaubt wird. In weiterer Folge haben wir dann Facebook-Sitzungen analysiert, die unseren Tor-Server verlassen haben und für FiTM Angriffe missbraucht werden hätten können. Die Anzahl der möglichen FiTM Angriffskeime bildete in Folge die Grundlage unserer Angriffssimulation. Hierbei verwendeten wir ein Spam-zu-Phishing-Verhältnis von 70 zu 30 Prozent.

Während eines Zeitraums von 14 Tagen konnten wir rund sechs Millionen HTTP-Anfragen über unseren Tor-Exit-Knoten zählen. Facebook war die am häufigsten nachgefragte Domain und insgesamt für 7,68 Prozent aller Anfragen verantwortlich. Das am zweithäufigsten abgefragte soziale Netzwerk war Orkut das rund 0,49 Prozent aller HTTP-Anfragen verursachte. Wir konnten in unserem Experiment rund 4267 einzigartige Facebook-Sitzungen beobachten, die für Friend-in-the-Middle-Angriffe hätten übernommen werden können.

Tor

Das Tor-Netzwerk ist ein weit verbreitetes Anonymisierungs Netzwerk, das Nutzer-IP-Adresse im Internet verschleiert.

Session hijacking

Nennt man das Übernehmen einer fremden Benutzer-Session, oftmals indem man Datenverkehr abfängt und vortäuscht, der legitimierte Benutzer zu sein.

Im Internet

- *http://www.social-engineer.org/framework/Social_Engineering_Framework*
- *http://www.sba-research.org/wp-content/uploads/publications/FITM_InternetComputing_preprint.pdf*
- *http://www.eff.org/https-everywhere*
- *http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.61.9231&rep=rep1&type=pdf*

(Paper „Social Phishing“ von Jagatic el. al.)

Unsere Simulationsergebnisse ergaben, dass sich mit diesen rund 4000 FiTM Angriffskeimen mit drei Iterationen rund 300.000 Benutzer mit sozialen Spam angreifen ließen. Wir haben dabei die Erfolgswahrscheinlichkeit des Phishingangriffs mit rund 30 Prozent angenommen, was deutlich unter dem von Jagatic et. al. in „Social Phishing“ (siehe Links) empirisch festgestellten Wert von rund 72 Prozent liegt.

Zusammenfassung

Soziale Netzwerke eröffnen Angreifern neue Möglichkeiten des Social Engineerings, da die Beschaffung der Hintergrundinformation wesentlich erleichtert wird. Dabei werden oft Freundschafts-/Vertrauensverhältnisse ausgenutzt, um u.a. die Glaubhaftigkeit von Phishing.- und Spamnachrichten zu erhöhen. Zum einen kann durch die digitale Verfügbarkeit der persönlichen Information Social Engineering automatisiert werden, zum anderen werden klassische Attacken effizienter. Die Betreiber sozialer Netzwerke versuchen den Pool an persönlichen Daten bestmöglich gegen Zugriff von Unbefugten zu schützen. In diesem Artikel zeigen wir jedoch, dass sich diese Sicherheitsmechanismen mit relativ einfachen Mitteln aushebeln lassen, in unserem Fall auf Basis der fehlenden HTTPS-Verschlüsselung. Bei Facebook gibt es mittlerweile die Möglichkeit HTTPS zu aktivieren (standardmäßig deaktiviert), bei vielen anderen Betreibern helfen momentan nur spezielle Browsererweiterungen, wie bspw. „HTTPS-Everywhere“.

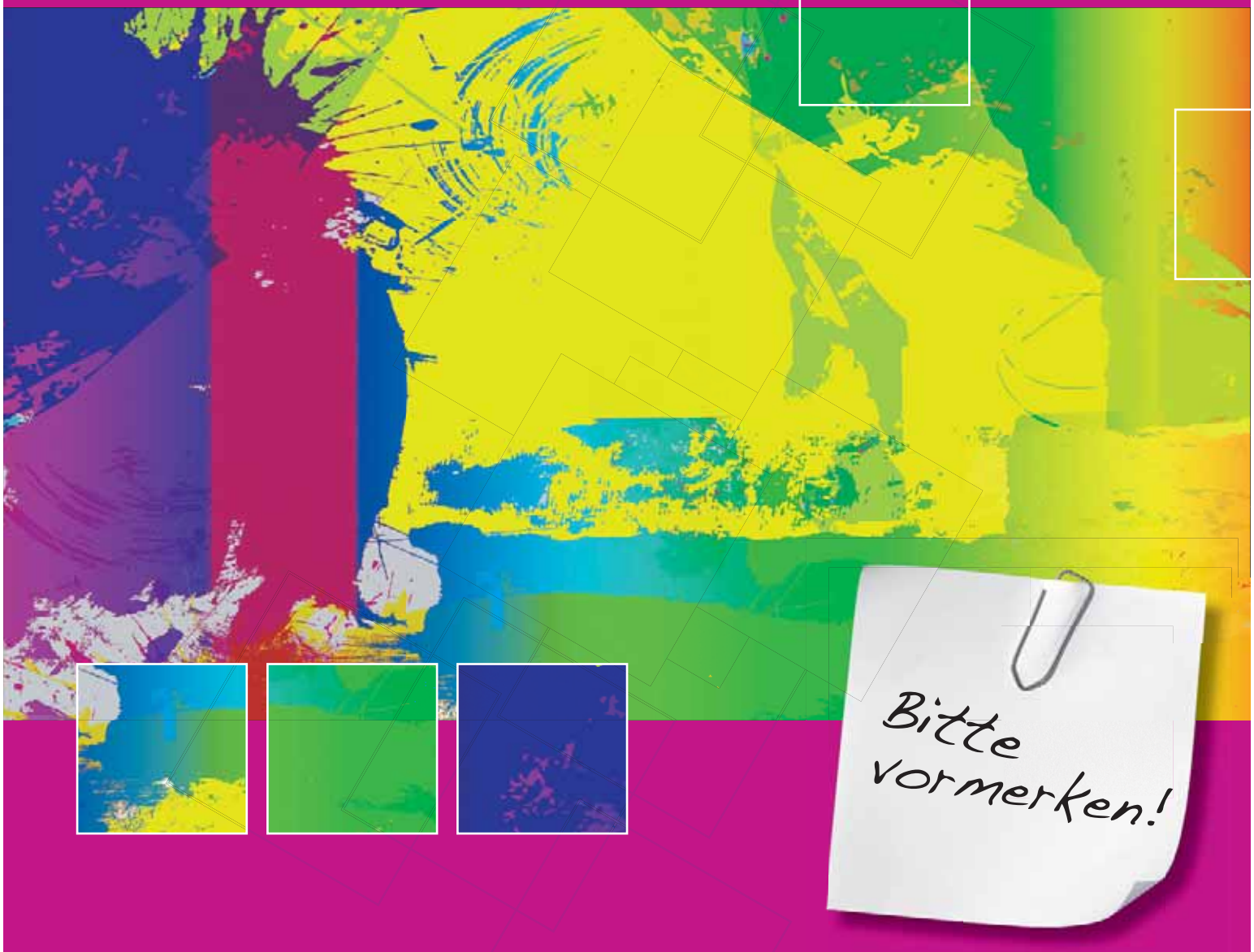
MARKUS HUBER UND PETER KIESEBERG

sind Forscher bei SBA Research, einem gemeinnützigen Forschungszentrum mit Themenschwerpunkt IT-Sicherheit in Wien.

Kontakt: mhuber@sba-research.org / pkieseberg@sba-research.org

Website: www.sba-research.org

itsecurity 2011



Gefahren erkennen, analysieren und Maßnahmen einleiten

Konferenz: 16. bis 18. Mai 2011 in München

www.it-security-2011.de

Nur eine spezielle IT-Haftpflichtversicherung sichert den IT-Freelancer optimal gegen seine beruflichen Haftungsrisiken ab

Matthias Talpa

Kleinste Programmierfehler, ein falsches Wort in der Google Adwords Kampagne oder die nicht erlaubte Verwendung von Bild- und Tonelementen auf der Website – all das sind Risiken, denen IT-Experten ausgesetzt sind. Was oft als nicht risikoreich abgetan wird, kann jedoch existenzbedrohende Nachwirkungen haben. Schutz dagegen bietet eine IT-Haftpflichtversicherung.

IN DIESEM ARTIKEL ERFAHREN SIE...

- wie sich IT-ler am optimalsten vor beruflichen Haftungsrisiken schützen

WAS SIE VORHER WISSEN SOLLTEN...

- kein spezielles Vorwissen

„Aus Schaden wird man klug", sagt ein altes Sprichwort. Was aber, wenn der Schaden die Existenz kostet? Besonders ärgerlich ist es auch, wenn man sich gut versichert glaubt, die Versicherung den Schaden aber wegen einem „Leistungsausschluss" im „Kleingedruckten" der Versicherungsbedingungen nicht bezahlt! Dabei sind sich viele IT-ler nicht bewusst, welchen Risiken sie in ihrem Arbeitsalltag ausgesetzt sind und was alles von der Versicherung abgedeckt sein sollte, um wirklich sorglos gegen alle möglichen Schadenfälle gewappnet zu sein.

Insbesondere bei Freiberuflern und kleinen IT-Dienstleistern ist häufig festzustellen, dass Haftpflichtrisiken und die damit verbundenen Versicherungsthemen nicht ausreichend beachtet werden. So mancher schließt eine konventionelle Betriebs- oder Bürohaftpflichtversicherung ab, bei der echte Vermögensschäden nicht mitversichert sind und der IT-Experte weiß nicht, dass eine solche Versicherung die am häufigsten auftretenden Schadenfälle im IT-Bereich gar nicht abdeckt.

Die unterschiedlichen Haftpflichtversicherungen

Grundsätzlich gibt es zwei Arten der Haftpflichtversicherungen, die für Unternehmen in Frage kommen.

1. Die Betriebshaftpflicht deckt generell die Haftpflichtansprüche, die einem Dritten durch die betriebliche Tätigkeit eines Unternehmens schuldhaft verursacht wurden. Nur die Eigenschaften und Rechtsverhältnisse, die der Versicherungsnehmer bei Vertragsabschluss angibt, fallen unter den Versicherungsschutz. Eine normale Betriebshaftpflichtversicherung versichert nur Ansprüche, die aufgrund von Personen- oder Sachschäden und daraus folgenden Vermögensschäden, wie z. B. Erwerbsausfall des Geschädigten (= Vermögensschaden) nach einem vom Versicherten verschuldeten Unfall (= Personenschaden) gestellt werden. Sie greift also nicht bei echten Vermögensschäden (z.B. Programmierfehler, Urheberrechtsverletzung, etc.), die nicht im Zusammenhang mit einem vorangegangenen Sach- oder Personenschaden entstehen.
2. Die Vermögensschadenhaftpflichtversicherung schützt vor Schäden, die durch Fehler bei der Ausübung der beruflichen Tätigkeit von IT-Experten im Vermögen anderer entstehen. Sie gilt nicht für Personen- oder Sachschäden, sondern für Vermögensschäden beispielsweise durch falsche Auskünfte, Beratung, Begutachtung etc. Dies betrifft vor allem Berufsgruppen, die im Dienstleistungsbereich tätig sind.

Konventionelle Haftpflichtangebote nicht ausreichend für den IT-Dienstleister

Für eine bedarfsgerechte Absicherung des IT-Dienstleisters ist es wichtig, dass in einer speziellen IT-Haftpflichtversicherung sowohl das Betriebshaftpflichtrisiko,

als auch die weitaus wichtigeren Vermögensschäden umfassend versichert sind.

Diese Berufshaltpflichtversicherung für IT-Experten muss die Risiken und alle Schäden (Personen-, Sach-, und Vermögensschäden) abdecken, die sich aus deren beruflichen Tätigkeit ergeben können.

10 Empfehlungen zur optimalen IT-Haftpflicht

Oft ist es schwierig, die richtige Versicherung für IT-Experten zu finden, die einen umfassenden Schutz bietet und bezahlbar ist. Dabei sind viele Aspekte zu beachten. Die folgende Check-Liste hilft, die optimale IT-Haftpflichtversicherung zu finden:

1. **Bedingungswerk prüfen**
   Wichtig ist, zu prüfen, ob die bestehende Versicherungspolice eine weitgehende Deckung von Vermögensschäden bei Auftraggebern bietet. Dazu ist es nötig, das Bedingungswerk des Versicherers im Detail zu analysieren. Es muss einfach, umfassend und transparent geschrieben auch dem Versicherungslaien klarmachen, in welchen Fällen der Versicherer leistet und in welchen Fällen nicht.
2. **Alle IT-Tätigkeiten absichern** (so genannte „offene Deckung“)
   Bedarfsgerechter Versicherungsschutz muss möglichst alle Tätigkeiten des IT-Freelancers und nicht nur eine abschließende Aufzählung von versicherten Tätigkeiten umfassen. Auch neu hinzukommende Tätigkeiten sollten ohne Einschränkung mitversichert sein. Wichtig für Unternehmen mit Tochtergesellschaften und unselbständigen Niederlassungen ist deren beitragsfreie Mitversicherung.
3. **Alle Schadenarten absichern**
   Versichert sollten grundsätzlich alle drei Schadenarten (Personen-/ Sach-/ Vermögensschäden) sein, die aufgrund der beruflichen Tätigkeit des IT-Freelancer entstehen oder durch dessen Betriebsstätte ausgelöst werden (z.B. Feuer in Ihrem Firmengebäude, das auf die Nachbarschaft übergreift).
4. **Erfüllungsfolgeschäden mitversichern**
   Der Versicherungsschutz sollte auch alle Folgeschäden aus Schlecht- oder Nichterfüllung eines Vertrages beim Auftraggeber sowie Folgen mangelhafter Produkte oder Dienstleistungen, zum Beispiel Betriebsausfallschäden und entgangene Gewinne, abdecken.
5. **Vertragsabschluss, Serviceleistungen und Validierung online**
   Eine effiziente Abwicklung vom Vertragsabschluss, über die Mitteilung geänderter Daten bis hin zur Schadenmeldung und auch die Vertragskündigung an einer zentralen Stelle schafft Sicherheit und hilft wertvolle Zeit sparen. Deshalb sollten der Vertragsabschluss und die Vertragsverwaltung anwenderfreundlich online möglich sein. Nur so entstehen keine zeitlichen und örtlichen Abhängigkeiten. Auch die Überprüfung der Gültigkeit des Versicherungsschutzes durch Auftraggeber (Validierung), sollte auf einfache Weise online möglich sein. Die Online-Abwicklung ist nicht nur für den Versicherungskunden bequemer, sondern hilft dem Versicherer auch Verwaltungskosten einzusparen, wodurch der Beitrag für den Versicherungsnehmer kostengünstiger angeboten werden kann.
6. **Fester Selbstbehalt**
   Im Schadenfall hat der Versicherte einen Teil der entstandenen Kosten selbst zu tragen. Dadurch können Versicherungsbeiträge günstiger kalkuliert werden. Der sogenannte Selbstbehalt sollte über die gesamte Vertragslaufzeit konstant und die finanzielle Belastung des Versicherten im Schadenfall kalkulierbar sein.
7. **Eigenschäden bedenken**
   Eigenschäden des Versicherungsnehmers in Form von Unredlichkeit eigener Mitarbeiter (Betrug, Untreue, Unterschlagung) ihm gegenüber sind bei einer guten IT-Haftpflichtversicherung ebenfalls abgedeckt. Sogar Eigenschäden, die für den IT-Dienstleister selbst aus dem berechtigten Rücktritt des Auftraggebers von einem gescheiterten IT-Projekt entstehen, sind bei guten Angeboten im Versicherungsumfang ohne Mehrbeitrag enthalten.
8. **Aufgabe des Versicherers: Passiver Rechtsschutz**
   Unter passivem Rechtsschutz im Rahmen einer IT-Haftpflichtversicherung versteht man, dass der Versicherer für den IT-Experten einen Rechtsstreit führt, wenn zum Beispiel unberechtigte Ansprüche auf Schadenersatz gegen ihn gestellt werden. Dabei sollte der Haftpflichtversicherer die ggf. anfallenden Verfahrens- und Gerichtskosten übernehmen. Stellt sich im Rechtsstreit heraus, dass den IT-Freelancer ein Verschulden trifft, begleicht der Versicherer darüber hinaus natürlich auch den Schaden im versicherten Umfang.
9. **Weltweite Absicherung**
   Es sollte darauf geachtet werden, dass der Versicherungsschutz weltweit gilt, auch in den USA und Kanada.
10. **Vorumsätze mitversichern**
    Schäden, die nach Beginn der Versicherung eintreten, sollten ohne zeitliche Begrenzung auch dann versichert sein, wenn die Tätigkeiten bereits vor Versicherungsbeginn erbracht wurden.

MATTHIAS TALPA

Matthias Talpa ist Geschäftsführer der Firma Konzept und Verantwortung Versicherungsmakler GmbH, die seit 2004 das Versicherungsportal für IT-Experten www.KuV24.de betreibt, wo IT-Dienstleister online speziell für sie entwickelte Versicherungen abschließen können.

Die Cloud nimmt es mit der Spamflut auf

Willem Vooijs

Spam ist für Unternehmen mehr als ein Ärgernis: Die Abwehr der Nachrichtenflut kostet Ressourcen und Bandbreite. Gelangen Spam-E-Mails durch den Filter, geraten Unternehmensdaten in Gefahr. Abhilfe schaffen Managed E-Mail Services aus der Cloud, die Spam und Malware dem Firmennetz fernhalten.

IN DIESEM ARTIKEL ERFAHREN SIE…

- Wie Sie mit Hilfe einer Managed E-Mail Security Lösung Spam--E-Mails und Viren dem Unternehmensnetz wirkungsvoll fernhalten, damit das Sicherheitslevel erhöhen und gleichzeitig Bandbreiten schonen sowie die Produktivität erhöhen.

WAS SIE VORHER WISSEN SOLLTEN…

- Rund 90 Prozent des gesamten E-Mail-Aufkommens ist Spam. Die überflüssige Post ist nicht nur lästig, sondern kostet auch Zeit, Bandbreiten und bringt im Falle infizierter Mails oder einer Phishing Attacke Unternehmensdaten in Gefahr – oft unbemerkt.

Die Zahl ist so hoch, dass sie beinahe keinerlei Bezug mehr zur Realität hat: 183 Milliarden Spam-E-Mails werden jeden Tag verschickt. Das belegt ein Report von Commtouch Software. Auch andere Analysen sprechen eine klare Sprache: Die Spam-Menge ist gigantisch. Der Anteil am weltweiten E-Mail-Verkehr liegt – je nach Statistik – zwischen 85 und 98 Prozent. Davon stammen wiederum

Abbildung 1. *KMUs erhalten mit Avira Managed Email Security (AMES) einen Service aus der sicheren Cloud, der E-Mails filtert und auf Schädlinge überprüft noch bevor sie den Server beziehungsweise das Unternehmensnetz erreichen können. Für den Service fallen weder Einrichtungs- noch Lizenzkosten an; der Anwender bezahlt lediglich eine Gebühr von knapp zwei Euro pro Monat und Postfach.*

beinahe 100 Prozent aus Botnetzen. Also Armeen aus Millionen von gekaperten PCs in Haushalten und Büros, die quasi zum Nulltarif für die Hintermänner Spam versenden.

Damit steht dann auch fest, dass Spam auf absehbare Zeit ein großes Problem bleiben wird, denn noch können Online-Kriminelle Geld damit verdienen. Unternehmen sind demnach auch in Zukunft auf wirksame Spam-Abwehr angewiesen. Die unerwünschten Nachrichten sind nicht nur einfach lästig. Sie können auch eine Gefahr für Unternehmensdaten darstellen. Und zwar dann, wenn es sich beispielsweise um eine Phishing-Kampagne handelt und unbedarfte Mitarbeiter Login-Daten eines Firmenaccounts auf der Phishing-Seite preisgeben.

Unangenehm ist auch, dass Spam Geld kostet. Denn IT-Abteilungen in Unternehmen müssen sich intensiv mit dem Problem auseinander setzen, was negativ zu Buche schlägt und die IT-Profis von wichtigen Aufgaben abhält. Je nach Unternehmensgröße und Anzahl der Postfächer kann die einströmende Spamflut die verfügbare Bandbreite schmälern – und nicht zuletzt die Produktivität der Mitarbeiter verringern.

Spam muss ganz weit draußen bleiben

Daher ist es ratsam, unerwünschte E-Mails gar nicht erst bis zum internen Spam-Filter oder gar E-Mail-Server vorzulassen. Vielmehr empfiehlt sich, den Mailverkehr von einem sicheren Cloud-Service filtern und nur die sicheren Nachrichten an den Unternehmensserver weiterleiten zu lassen.

Die Spambekämpfung „in-the-cloud“ erfordert keinerlei Softwarekomponenten auf den Unternehmens-PCs – oder Netzwerkkomponenten. Vielmehr wird sämtlicher eingehender – und auch der aus dem Unternehmensnetz versandte – E-Mail-Verkehr per verändertem MX-Eintrag, also einem Wert im DNS (Domain Name System), ans Rechenzentrum des Anbieters geschickt. Dort wird die elektronische Post auf Spam bzw. Schädlinge untersucht, ohne die Ressourcen des Anwenders oder dessen Netzwerkbandbreite in Anspruch zu nehmen. Nur die für unbedenklich befundenen Nachrichten erreichen letztendlich den unternehmenseigenen E-Mail-Server.

Ausgelagert und dennoch unter Kontrolle

Durch das Verlagern der Spam- und Virenabwehr in die Rechenzentren eines externen IT-Sicherheitsexperten, profitieren Unternehmen von einer stets aktuellen, bewährten Sicherheitslösung, denn der Service wird laufend mit Updates zum Schutz vor Malware versorgt.

Beim gemanagten Avira E-Mail Security Service (AMES) kommen hierbei beispielsweise unterschiedliche Technologien zum Einsatz, wie ein heuristischer Scanner, der Spam bzw. neue Bedrohungen anhand der Schemata und Verhaltensweisen im E-Mail-Verkehr aufspürt. Auf diese Weise können infizierte E-Mails ausfindig gemacht werden, noch bevor ein neues Virenupdate für eine lokal installierte Antiviren-Software verfügbar ist.

Das Plus an Sicherheit geht nicht mit einem Kontrollverlust einher, denn die IT-Administratoren eines Unter-

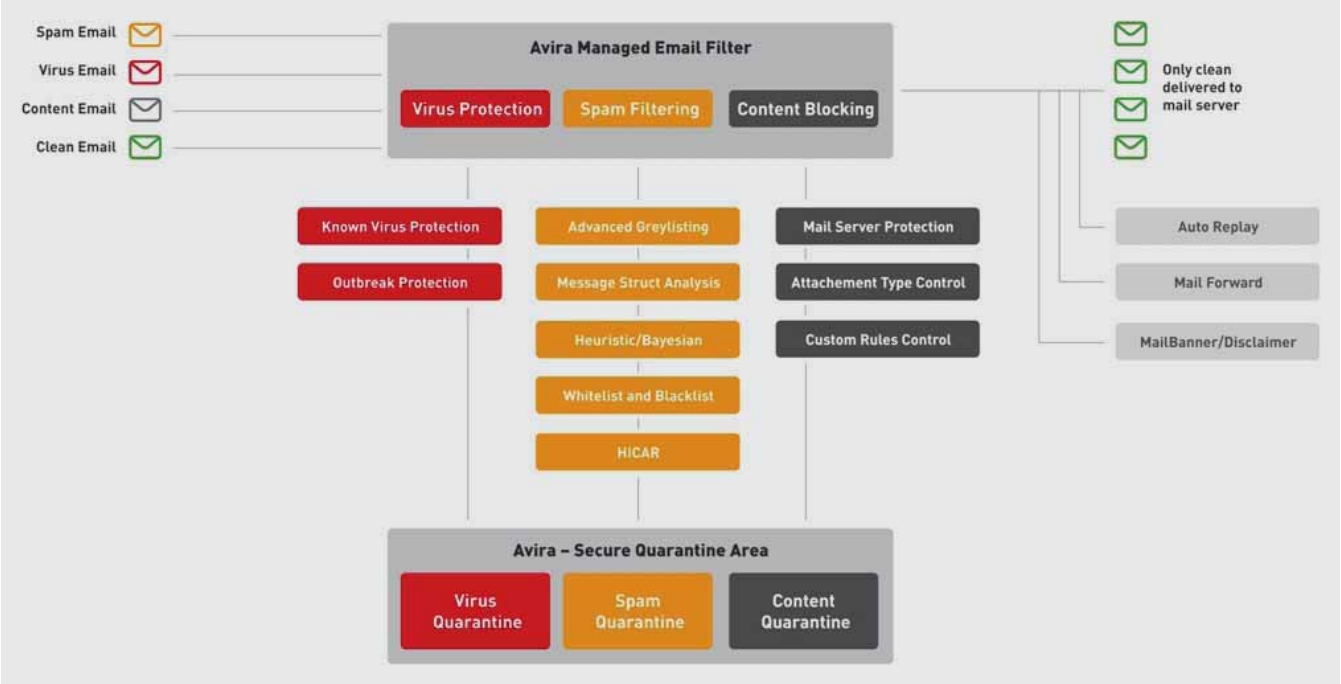


Abbildung 2. *AMES bietet Schutz vor Spam, Viren und anderen Bedrohungen und leitet ausschließlich die sicheren Nachrichten an das Firmennetz weiter. Infizierte E-Mails und Spam-Nachrichten werden in den Quarantäne-Bereich verschoben, damit sie im Unternehmen keinen Schaden anrichten.*

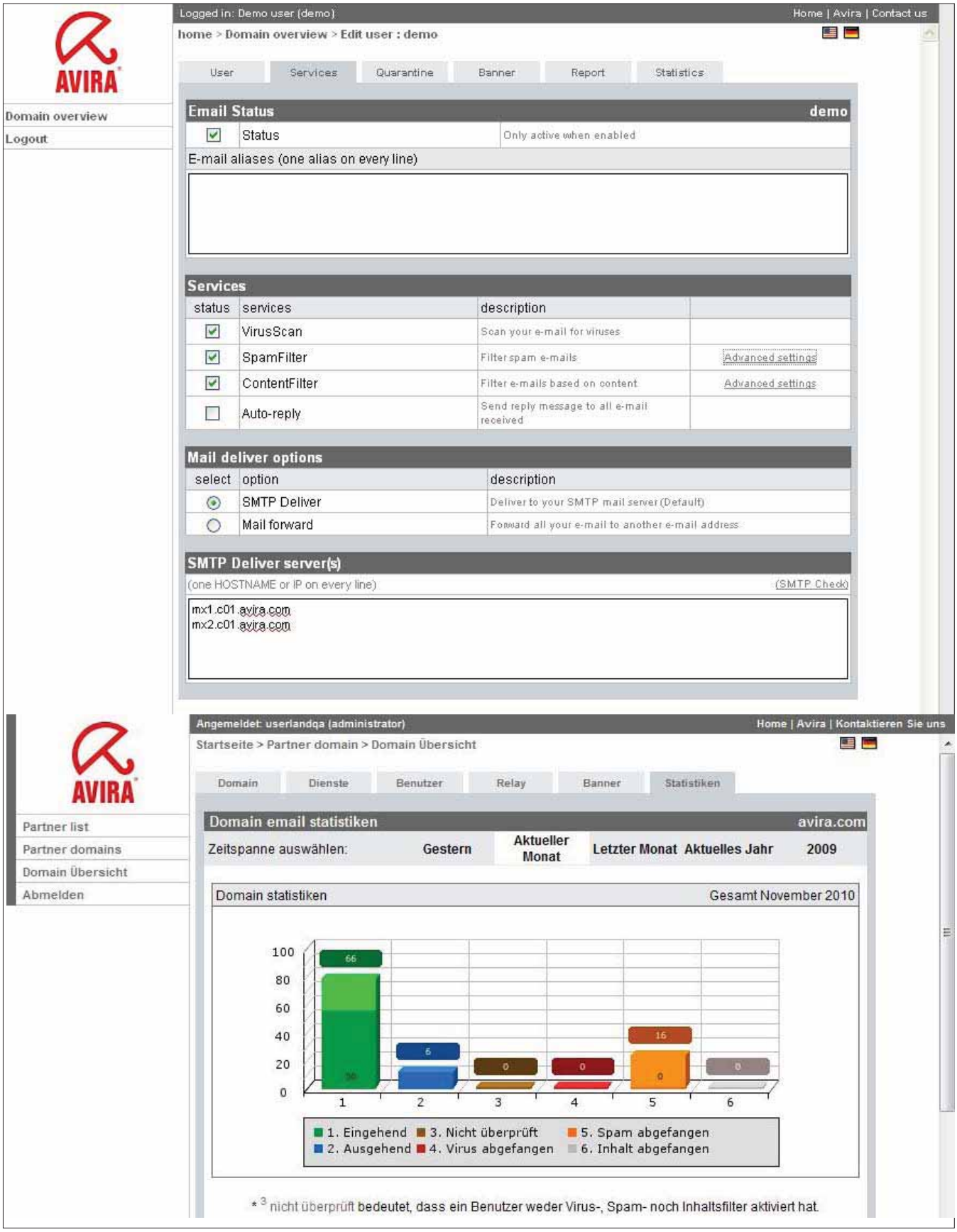


Abbildung 3. *Die komplette Kontrolle über das System inklusive detaillierter Filterregeln ermöglicht Avira über das intuitive Benutzerportal MyAccount.avira.com. Darüber lassen sich nutzerabhängige Einstellungen und Rechte definieren. Beispielsweise können bestimmte Arten von Nachrichten, Inhalten oder Anhängen blockiert oder manuell freigegeben werden. Hilfestellung erhalten Unternehmen bei Bedarf über den deutschsprachigen Avira Support.*

nehmens haben in der Regel über ein Web-Portal alle Einstellungen, Berichte, Statistiken und die in Quarantäne beförderten Nachrichten im Griff. Hierüber sollten sich nutzerabhängige Einstellungen und Rechte definieren lassen – vom Administrator über Gruppen bis hin zu einzelnen Anwendern. So können bestimmte Arten von Nachrichten, Inhalten oder Anhängen blockiert oder manuell freigegeben werden.

Praktisch ist ein Cloud-basierter Spam-Filter auch dann, wenn ein Unternehmen einmal vom Internet getrennt werden sollte. Dann kann der Dienstbetreiber als Zwischenspeicher dienen und die aufgelaufenen Nachrichten ausliefern, sobald das Netzwerk des Kunden wieder erreichbar ist.

Die IT-Profis der Unternehmen profitieren vom gemanagten Security Service gleich doppelt: Zum einen können sie ihr Netzwerk verlässlich sauber halten – zum Beispiel garantiert Avira per SLA die Abwehr sämtlicher bekannter Malware und mindestens 99,9 Prozent aller Spam-Nachrichten. Zum anderen bleibt ihnen mehr Zeit für andere Aufgaben, die nicht von externen Servicepartnern übernommen werden können.

Wirtschaftlich und granular

Somit bieten Managed E-Mail Security Services also ein erhöhtes Sicherheitslevel für Unternehmen. Gleichzeitig werden Infrastruktur sowie Mitarbeiter entlastet, die Performance gesteigert und Kosten gespart. Außerdem sprechen die niedrigen Anlaufkosten für das Outsourcing: Es fallen keine Lizenzkosten für lokal installierte Softwareprodukte oder Appliances an. Der Kunde zahlt zumeist lediglich eine Gebühr pro Monat und Postfach. Auch ein auf einzelne Abteilungen oder E-Mail-Domänen eines Unternehmens beschränktes Absichern ist machbar. So lassen sich die Kosten für die Spam- und Malwareabwehr noch bedarfsgerechter steuern.

Vorteilhaft ist es, wenn der Anbieter des Anti-Spam-Dienstes eine kostenfreie Testphase ermöglicht. Aufgrund der geringen Einstiegshürde – das Ändern des MX-Eintrages im DNS ist eine Sache von wenigen Minuten und kann meist ohne Zutun des Service Providers vom Anwender selbst erledigt werden – herrschen ideale Voraussetzungen, um sich selbst ein Bild von der Leistungsfähigkeit des Cloud-Dienstes zu verschaffen, ohne hierfür technische Klimmzüge absolvieren zu müssen.

WILLEM VOOIJS
Der Autor ist Product Manager Managed Services bei Avira

BESPRECHUNG DES MULTIMEDIALEN HACKING-KURSES

Die Hacking School vermittelt dem Leser Wissen rund um das Hacken. Das Ziel ist, den eigenen PC sicherer zu machen bzw. Sicherheitslücken zu entdecken und zu schließen. Das Hacking School Set beinhaltet ein Handbuch, eine DVD mit 19 Trainingsfilmen und eine CD mit dem Schulungsbetriebssystem. Das komplette Schulungsset kann für 87 EUR bestellt werden.

Pressemitteilung der Hacking School

Im Verlagsprogramm des CSH Verlags, Kwidzyn, Polen, erscheint dieser Tage die zweite, korrigierte und erweiterte Ausgabe des in Polen bereits äußerst erfolgreichen Hacking School Sets in deutscher Sprache. Das Schulungsset besteht aus einem Handbuch, einer DVD mit 19 Schulungsvideos (210 Minuten) sowie einem Schulungsbetriebssystem (Live-CD Linux mit der zum Kurs nötigen Software).

Der Kurs richtet sich an jeden, der sich von Hackerangriffen bedroht fühlt, frei nach dem Motto „...möchtest du einen Dieb fangen, denke wie einer..." Profitieren können von dem Werk sowohl ambitionierte Anfänger, die schon immer wissen wollten, welcher technische Hintergrund sich hinter dem Thema Hacking verbirgt, als auch professionelle Administratoren, die Sicherheitslücken in ihrem System aufdecken wollen.

Das Buch führt den Leser Schritt für Schritt sowohl in die grundlegenden als auch in die fortgeschrittenen Techniken des Hackings ein. 21 Kapitel auf 420 Seiten mit Informationen, Anwendungsbeispielen, aber auch Übungen, mit deren Hilfe man praktische Fähigkeiten erlernt. Jedes Kapitel stellt einen unabhängigen Abschnitt dar und behandelt ein ausgewähltes Thema.

Das Trainingsmaterial kann auf dem speziell vorbereiteten Trainingsbetriebssystem durchgespielt werden, welches von der CD startet und nicht installiert zu werden braucht. Zwei Minuten nach dem Start ist die Testumgebung für den Leser einsatzbereit. Es dient als überaus nützlicher Wegweiser und Begleiter zu sicherheits relevanten Aspekten des IT-Systemschutzes.

Was erwartet Sie in diesem Kurs:

- Die Wiederherstellung verlorener Passwörter
- Das Abfangen von Informationen in lokalen Netzwerken
- Das Abfangen von verschlüsselten Daten
- Angriff auf eine SSL-Sitzung
- Backdoor - die "Hintertür" als Tor zum System
- Dateien und Verzeichnisse mit Hilfe des Kernels 2.6 verstecken
- Angriffe vom Typ Buffer-Overflow
- Angriffe vom Typ Heap-Overflow
- Format-String-Angriffe
- Das Überschreiben des Datenstrom-Zeigers (File Stream Pointer Overwrite)
- Fehler im Systemkernel
- Die Verwendung des ICMP-Protokolls aus der Sicht des Hackers
- Identifizierung eines Netzwerkcomputers
- Netfilter im Dienste der Systemsicherheit
- Absichern des Betriebssystems Schritt für Schritt
- Sicherheitsscanner
- Kernelpatches zur Erhöhung der Sicherheit
- Intrusion Detection System (IDS)
- Angriff mit Hilfe eines Webservers
- Shellcode-Erstellung in der Win32-Umgebung

Zusammenfassung

Das Schulungsset "Hacking School" stellt eine fundierte und tiefgehende Einführung ins Hacking dar, sowohl für Anfänger als auch für fortgeschrittene Power-User. Wir empfehlen dieses Set jedem, der die ersten Schritte in die Welt des Hackens und der Computersicherheit wagt.

Der Kurs ist auch bei Amazon erhältlich.

Promotionscode nur für Leser der Zeitschrift **haking**
10% Rabatt: ***72888*** bei Kauf der Schulung

Bestellung des Schulungsexemplars
auf ***www.HackingSchool.de***

Netzwerk-Sicherheit – Schutz eines Netzwerks durch ein Check Point Security Gateway

Stefan Schurtz

Check Point Software Technologies Ltd. ist weltweit für seine Firewall- und VPN-Produkte bekannt, und stellt mit seiner noch recht neuen Software Blades eine sehr flexible Security Architektur für Unternehmen bereit.

IN DIESEM ARTIKEL ERFAHREN SIE…

- Wie man ein Check Point Security Managemet und Security Gateway in der Version R75 zum Schutz eines Netzwerks installiert und konfiguriert

WAS SIE VORHER WISSEN SOLLTEN…

- Kenntnisse in der System- und Netzwerk-Sicherheit
- Kenntnisse in der TCP/IP Netzwerktechnik

Einführung

Firewalls gelten als ein wichtiger Teil der IT-Infrastruktur und bilden den Übergang von einem unsicheren, nicht vertrauenswürdigen Netzwerk (z. b. dem Internet) in einen oder mehrere als sicher bzw. vertrauenswürdig geltenden Bereich eines (Firmen)-Netzwerkes.

Auch wenn die heutigen Firewall-Produkte immer sicherer zu werden scheinen, mit gehärteten Betriebs-

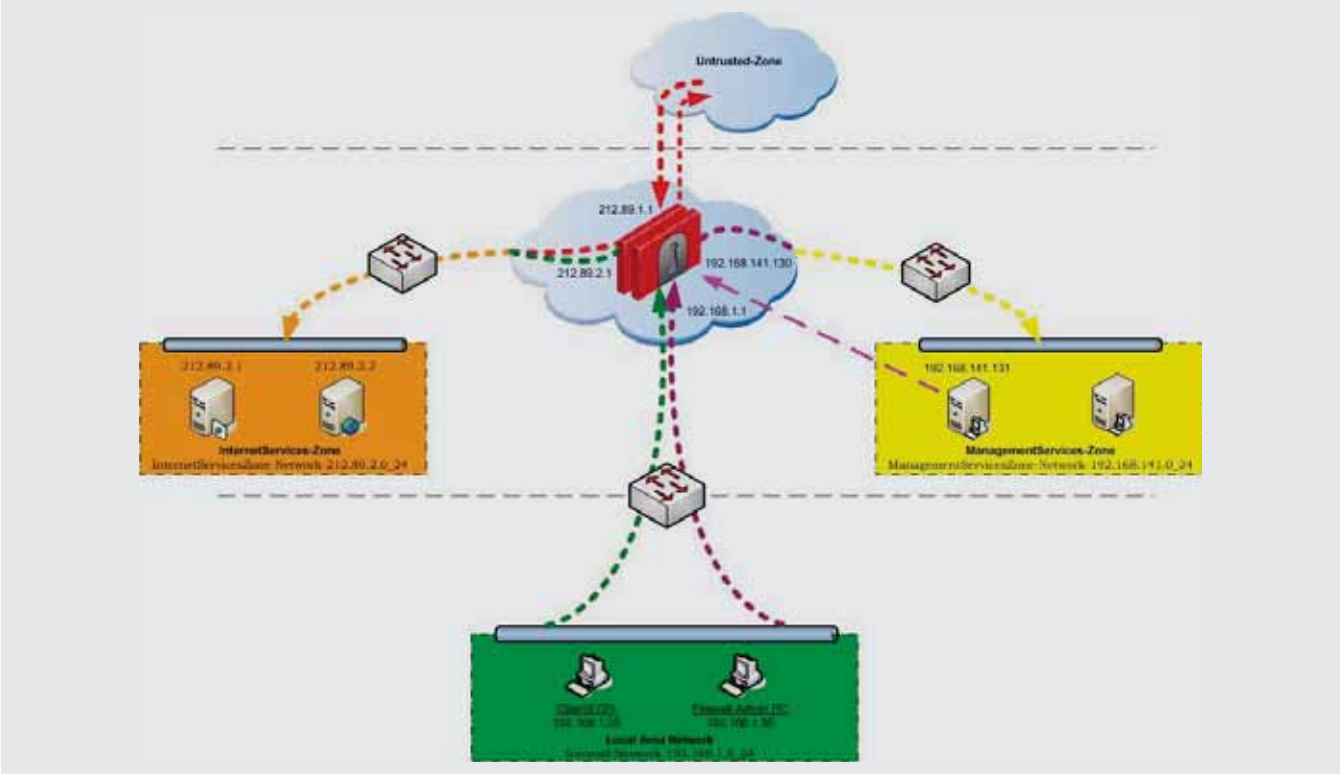


Abbildung 1. *Netzplan*

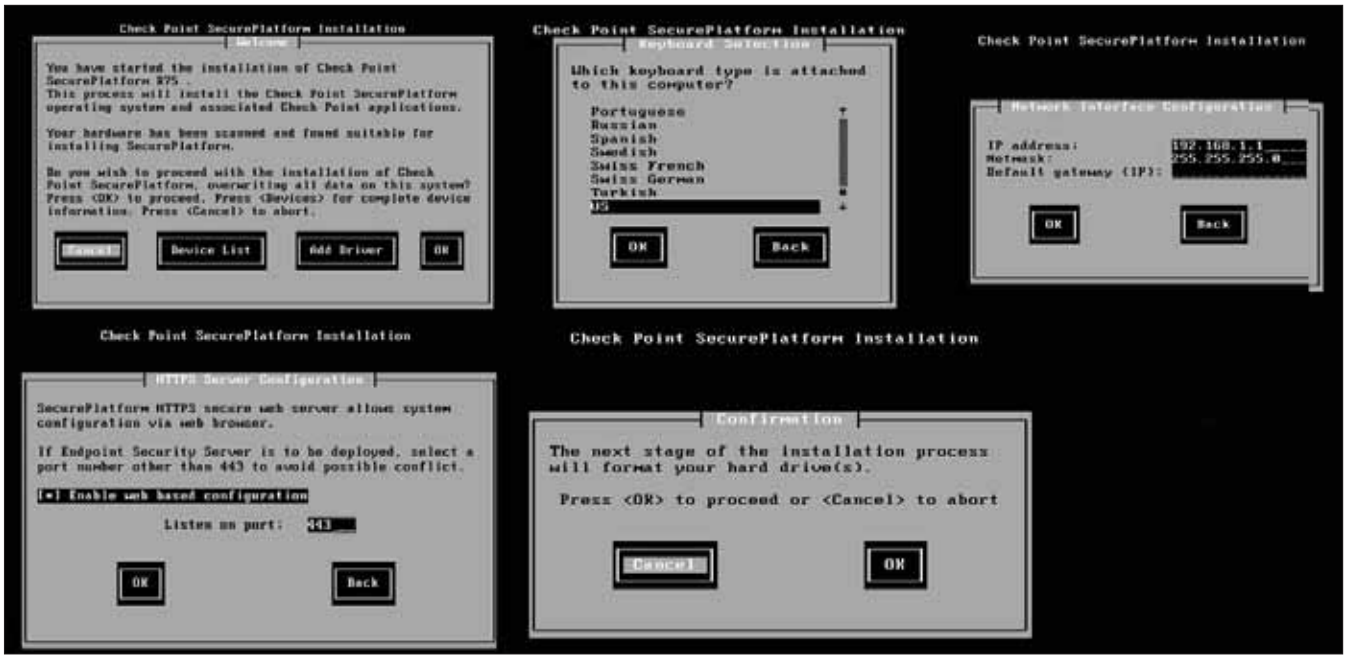


Abbildung 2. *Grundinstallation*

systemen daher kommen, steigt auf der einen Seite der Grad an Komplexität der zu schützenden Netzwerke und auf der anderen Seite, wachsen der Druck und Anforderungen an die Security-Administratoren. Schnell werden wichtige und nötige Dokumentationen und Standards „vergessen“ bzw. vernachlässigt und dann sind es gerade diese wichtigen Systeme die Fehlerkonfigurationen unterliegen, was wiederum dazu führen kann, dass selbst die beste und teuerste Firewall schnell ziem-

Abbildung 3. *Erster Login auf der WebGUI*

Abbildung 4. *First Time Configuration Wizard-Products*

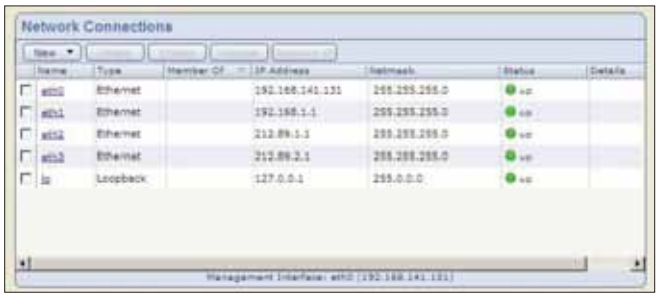


Abbildung 5. *Konfiguration der vorhanden Netzwerkinterfaces*

Abbildung 6. *Fingerprint des Security-Managements*

lich nutzlos wird und von findigen Angreifen schnell überwunden werden kann. Daher ist es für einen Security-Administrator ungemein wichtig den Überblick über das Regelwerk nicht zu verlieren, dieses so einfach wie nur möglich zu gestalten, sich eine strikte Vorgehensweise bzw. einen Standard für die Konfiguration von Objekten, Regeln und Zugriffsrechten zu überlegen, zu dokumentieren und einzuhalten. Ebenso sollte auch die Konfiguration der Firewall bzw. des Regelwerks selbst, den Administrator nicht vor eine zu große Herausforderung stellen und relativ „einfach" durchzuführen sein und nicht durch eine komplizierte Syntax und/oder unübersichtliche Regel-Konfiguration unnötig erschwert werden.

Check Point

Check Point Software Technologies Ltd. ist weltweit für seine Firewall- und VPN-Produkte bekannt, und stellt mit seiner noch recht neuen Software Blades eine sehr flexible Security Architektur für Unternehmen bereit. Durch diese Architektur ist es möglich Gateway bzw. Management schnell um zusätzliche Security-Module (wie z. b. Application Control Software Blade, Identity Awareness Software Blade, DLP Software Blade, Mobile Access Software Blade) zu erweitern und neuen Anforderungen anzupassen und in einem zentralen Management zu administrieren. Vergessen sollte man hierbei allerdings

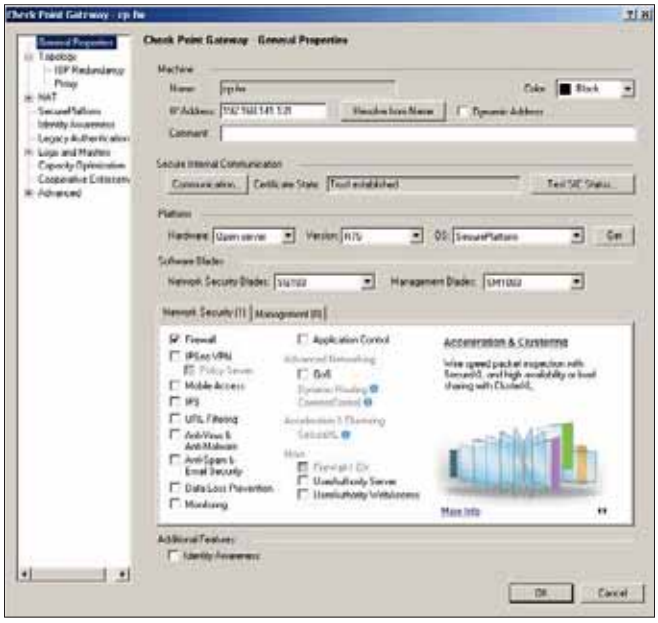


Abbildung 7. *Check Point Gateway Einstellungen*

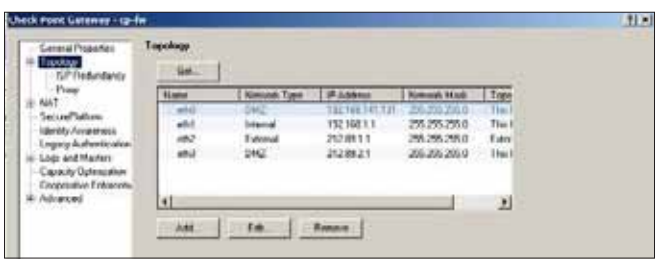


Abbildung 8. *Check Point Gateway Topology*

nicht, dass bei Check Point dies meist mit zusätzlichen (teils nicht unerheblichen) Kosten verbunden ist.

Dennoch bietet Check Point seinem Security Management und den damit verbundenen Werkzeugen (SmartDashboard, SmartTracker, SmartMonitor …) eine gute Möglichkeit mit Hilfe von Objekten (Networks, Groups, Nodes, Interoperable Devices) einen entsprechenden Standard zu etablieren und zu pflegen. Durch die mögliche Unterteilung des Regelwerks in Sektionen, dem Hin-

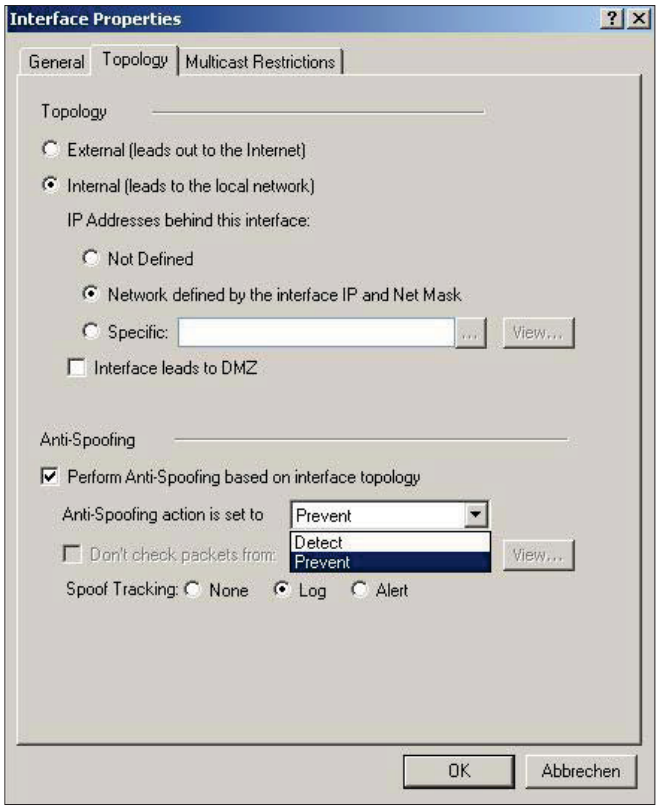


Abbildung 9. *Netzwerkinterface Einstellungen*

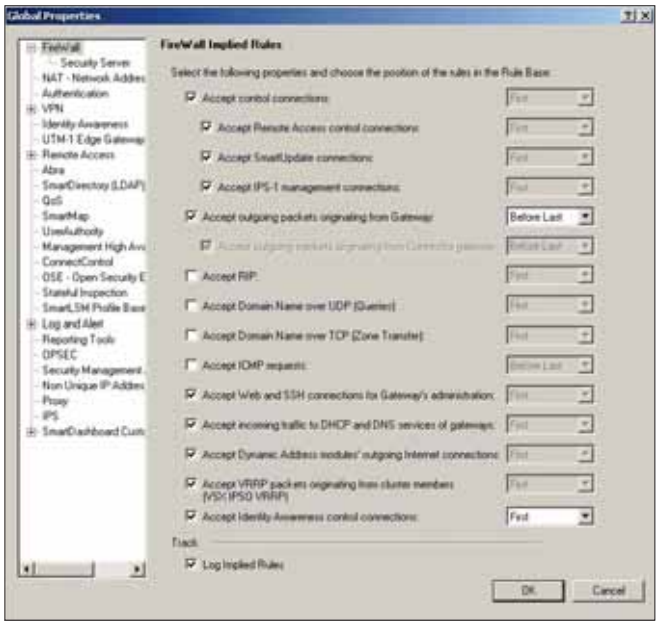


Abbildung 10. *„Implied Rules" Konfiguration*

terlegen von unterschiedlichen Farben für Objekte, der Benennung von Regeln und dem Hinterlegen von Kommentaren, erhält der Security-Administrator gute Hilfsmittel an die Hand, die Ihm helfen können, den Überblick über das Firewall-Regelwerk nicht vollends zu verlieren.

Übersicht

Der nachfolgende Artikel geht auf die Konfiguration eines Check Point Security Gateway, mit zentralem Management, auf der aktuellen Version R75 ein. Es wird gezeigt wie mit Hilfe des SmartDashboard ein Regelwerk zum Schutz eines (kleinen) Netzwerkes vor unerlaubten Zugriffen, mit zwei DMZ-Bereichen und des LANs (Abbildung1) konfiguriert werden kann. Das Ziel ist es hierbei, dass die Regeln für den jeweiligen Bereich unter eigenen Sektionen zusammengefasst werden, sämtlicher Traffic der über die Firewall läuft, sei es nun ein- oder ausgehend, explizit freigeben werden muss, damit nur die wirklichen benötigen Dienste erreichbar sind und jeder sonstige Traffic durch die Firewall geblockt wird. Bei der aktuellen Konfiguration nicht berücksichtigt werden weitere Sicherheitsmechanismen, wie beispielsweise Proxy/Content Filter, VPN-Zugänge, Mail-Gateway, da es den Rahmen des Artikels sprengen würde.

Installation

Die Installation eines Security Management und eines Security Gateway unterscheiden sich, bis zu der Auswahl der zu installierenden Produkte nicht voneinander. Nach dem Download des entsprechenden Image von der Check Point Website, in dem vorliegenden Fall „*Check_Point_R75.Splat.iso*“, dem Brennen auf eine DVD, startet nach dem Bootvorgang die Grundinstallation des auf Secure Platform basierenden Systems. Diese beinhaltet neben dem Festlegen des Keyboard Layouts, die Konfiguration eines Netzwerkinterface und des https-Ports für den Zugriff auf die WebGUI (Abbildung2). Nach einer letzten Bestätigung, wird im nächsten Installationsschritt die Festplatte formatiert und das Grundsystem installiert. Nach erfolgreicher Installation und einem Reboot steht das Webinterface per https, mit der konfigurierten IP und dem angegebenen Port, zur Verfügung.

Nach dem ersten erfolgreichen Login mit den Anmeldedaten „*Benutzer: admin;Passwort: admin*“, muss aus Sicherheitsgründen zunächst das Default-Password neu gesetzt werden (Abbildung3). Bei den nun folgenden Konfigurationsschritten werden übliche Systemeinstellungen, wie z. b. NTP, DNS, weitere IP-Adressen, Routing usw. abgefragt. Letztlich steht unter dem Punkt „*First Time Configuration Wizard-Products*“ (Abbildung4) die Entscheidung an, welche Aufgabe das System in Zukunft übernehmen soll, Security Gateway oder Check Point Management-Server. Wählt man hier nun den Punkt Security Management, stehen vor der endgültigen Fertigstellung noch die Konfiguration der „*Security Management GUI Clients*“ und der „*Security Management Administrators*“ an. Die Konfiguration eines Security Gateway unterscheidet sich insofern, da man hier nicht GUI-Clients bzw. Administratoren, sondern einen Activation Key für die Secure Internal Communication (kurz SIC) angeben muss, welcher Voraussetzung für die Kommunikation zwischen Security Gateway und Security Management ist.

Bevor man endgültig mit der Konfiguration per SmartDashboard beginnt, sollten noch die restlichen IPs (falls nicht schon bei der Installation geschehen) auf dem Gateway, per „*WebGUI -> Network -> Connections*“ konfiguriert werden (Abbildung5). Sind nun alle diese Schritte erfolgreich durchgeführt worden, wird im nächsten Schritt das SmartDashboard installiert und das Security Gateway in das Management aufgenommen.

SmartDashboard

Um sich nun mit dem Management zu verbinden muss das SmartDashboard für die jeweilige Version des Manage-

Abbildung 11. *Stealth Rule*

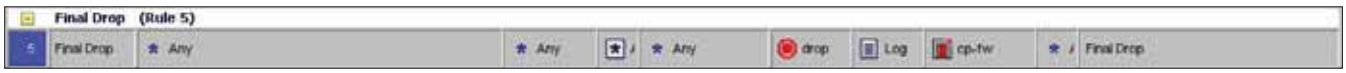


Abbildung 12. *„Final Drop"-Regel*

Abbildung 13. *Regeln zur Administration der Firewall-Nodes*

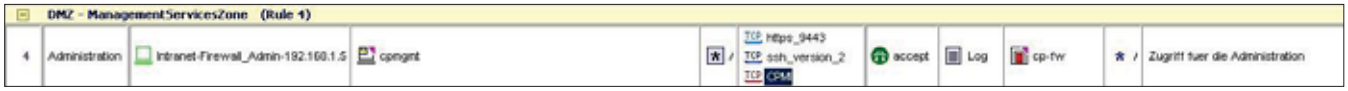


Abbildung 14. *Regeln zur Administration des Firewall-Managements*

Abbildung 15. *ICMP-Rules*

ment Server (hier R75) heruntergeladen und installiert werden. Dies kann entweder über die WebGUI *„Product Configuration -> Download SmartConsole Applications“* oder über die Check Point Website getan werden. Die Installation des SmartDashboard sollte niemanden vor eine allzu große Herausforderung stellen, daher wird hier nicht näher darauf eingegangen. Anzumerken wäre an dieser Stelle noch, dass es durchaus möglich ist mit einem Management-Server auf Version R75, ein Security Gateway in früherer Version (R71, R70, R65) zu administrieren, umgekehrt ist aber ein Security Gateway auf der Version R75 nicht von einem Management in einer älteren Version zu administrieren. Mit dem ersten Login per SmartDashboard wird ein Fingerprint (Abbildung6) abgefragt. Um die Korrektheit zu überprüfen, kann man den Fingerprint mit dem auf dem Management hinterlegten „*WebGUI -> Product Configuration -> Certificate Authority*“ vergleichen.

Einbinden in das Security-Management

Nach dem erfolgreichen Login per SmartDashboard fügt man auf der linken Seite über „*Network Objects -> Check Point -> Rechte Maustaste -> Security Gateway/Management*“ das Gateway ins Management ein. Dazu trägt man Namen und IP-Adresse des Gateway ein und unter dem Punkt „*Secure Internal Communication -> Communication (Certificate State steht zunächst auf: Uninitialized)“* den bei der Installation vergebenen Activation Key. Wenn hier alles funktioniert hat, steht der Certificate State nun auf „Trust established“ (Abbildung7) und es werden gleichzeitig die zuvor konfigurierten IPs in die Topology eingetragen (Abbildung8). In der Topology gelangt man per Doppelklick auf die einzelnen Interfaces in das sogenannte *Interface Properties*. Hier wird das Interface einem *Network Type* (Internal, External, DMZ) zugeordnet und das Anti-Spoofing konfiguriert (Abbildung9). Bei einem „Internal-Interface“ hat man die Möglichkeit zwischen *Network defined by the interface IP and Net Mask* oder *Specific* zu wählen. Wenn *Specific* ausgewählt wird, kann dort ein Netzwerk-Objekt oder gar ein Gruppen-Objekt hinterlegt werden, welches dann die Topology für das Interface bildet.

Regelwerk

Das Regelwerk auf einem Check Point Security Gateway wird von oben nach unten verarbeitet, d.h. genauer werden zuerst die sogenannten *Implied Rules* verarbeitet, welche man sich mit „*View -> Implied Rules“* im Re-

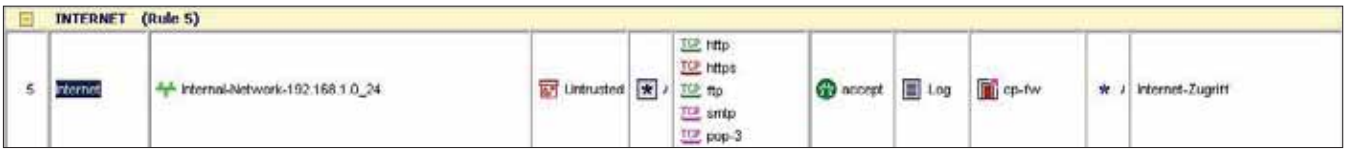


Abbildung 16. *Firewall-Regeln für den Zugriff auf das Internet*

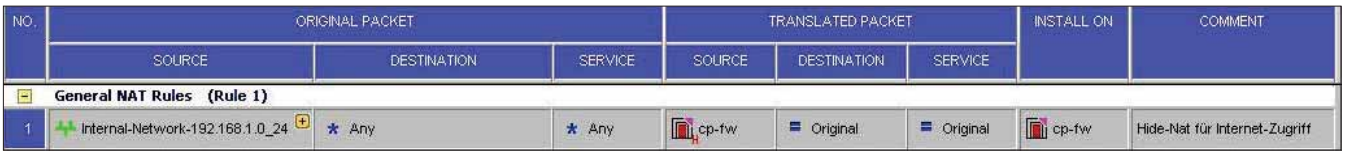


Abbildung 17. *General NAT Rules - „Hide-Nat“ für den Internet Zugriff*

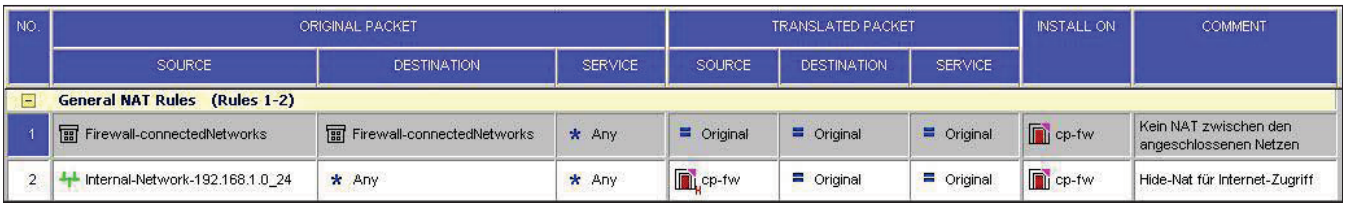


Abbildung 18. *General NAT Rules - Kein NAT zwischen den direkt verbunden Netzen*

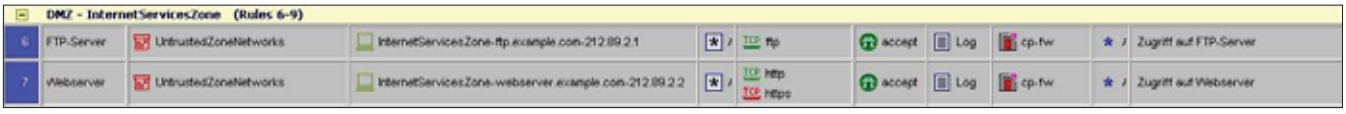


Abbildung 19. *Zugriff auf Web- und FTP-Server aus dem Internet*

Abbildung 20. *Zugriff auf Web- und FTP-Server aus dem LAN*

gelwerk anzeigen lassen kann. In den Implied Rules sind unter anderem *Control Connections für Remote Access, IPS-1* und *SmartUpdate* definiert, welche im Regelwerk nicht direkt zu bearbeiten sind. Unter dem Menüpunkt „*Policy -> Global Properties -> FireWall -> FireWall Implied Rules*“ (Abbildung10) können diese aktiviert, deaktiviert bzw. Logging und Reihenfolge eingestellt werden.

Für die Reihenfolge stehen folgende Möglichkeiten zur Auswahl: First, Before Last und Last. Wird eine Implied Rule als *First* definiert, kann diese nicht mehr von einer selbst erstellten Regel (Explicit Rule) überschrieben werden, da sie damit in der Verarbeitung des Regelwerks immer an erster Stelle steht. Bei der Definition *Before Last* wird die Regel, wie der Namen vermuten lässt, vor und mit der letzten Möglichkeit *Last* nach der letzten Regel (Implicit Drop Rule) verarbeitet, welche sämtliche Pakete verwirft und dazu führt, dass eine mit *Last* definierte Implied Rule keine Relevanz hat. Im Endeffekt bedeutet dies, wenn ein Paket bei der Verarbeitung auf eine Regel zutrifft, wird diese Regel angewandt, danach aber keine weitere, d.h. nur die erste zutreffende Regel wird auch tatsächlich ausgeführt.

Stealth Rule

Im ersten Schritt wird in dem Regelwerk unter dem Reiter „Firewall“ zunächst die Sektion “Stealth Rule“ über die Menüpunkte „*Rules -> Add Section Title -> Below/ Above*“ erstellt. Unter dieser folgt dann die erste selbst erstellte Firewall-Regel, welche sämtliche Anfragen an die Firewall selbst verbietet und dieser damit einen ge-

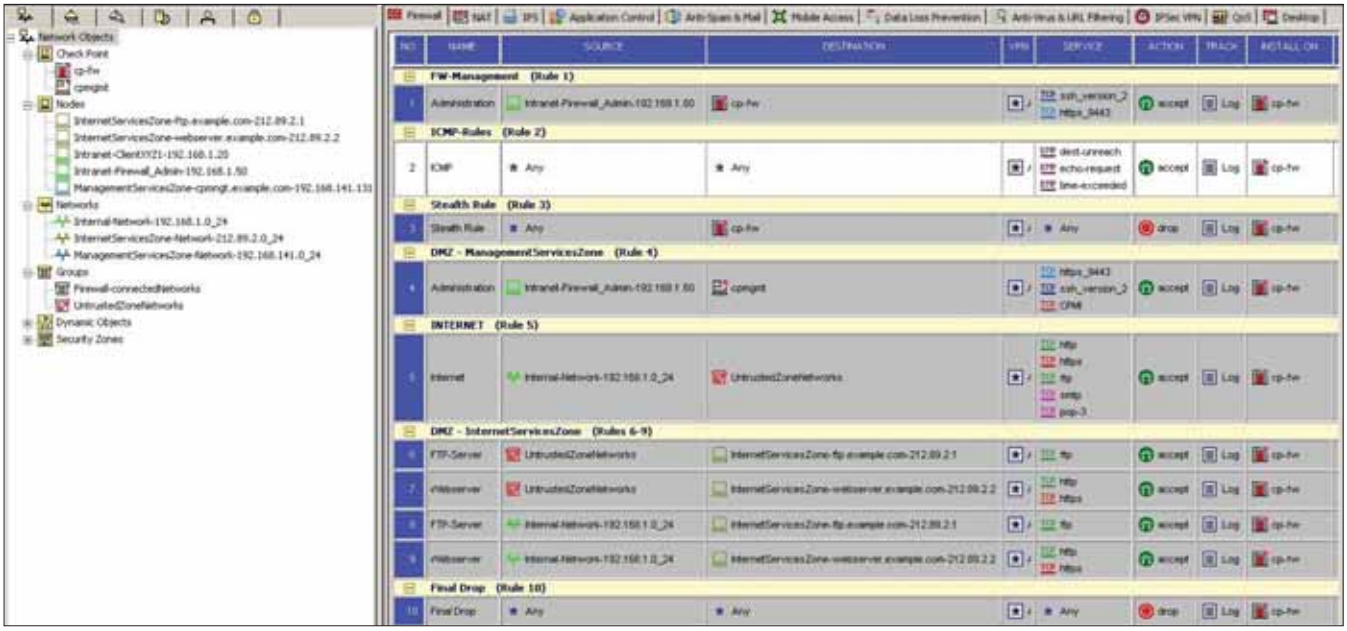


Abbildung 21. *Vollständiges Firewall-Regelwerk inkl. der erstellen Objekte*

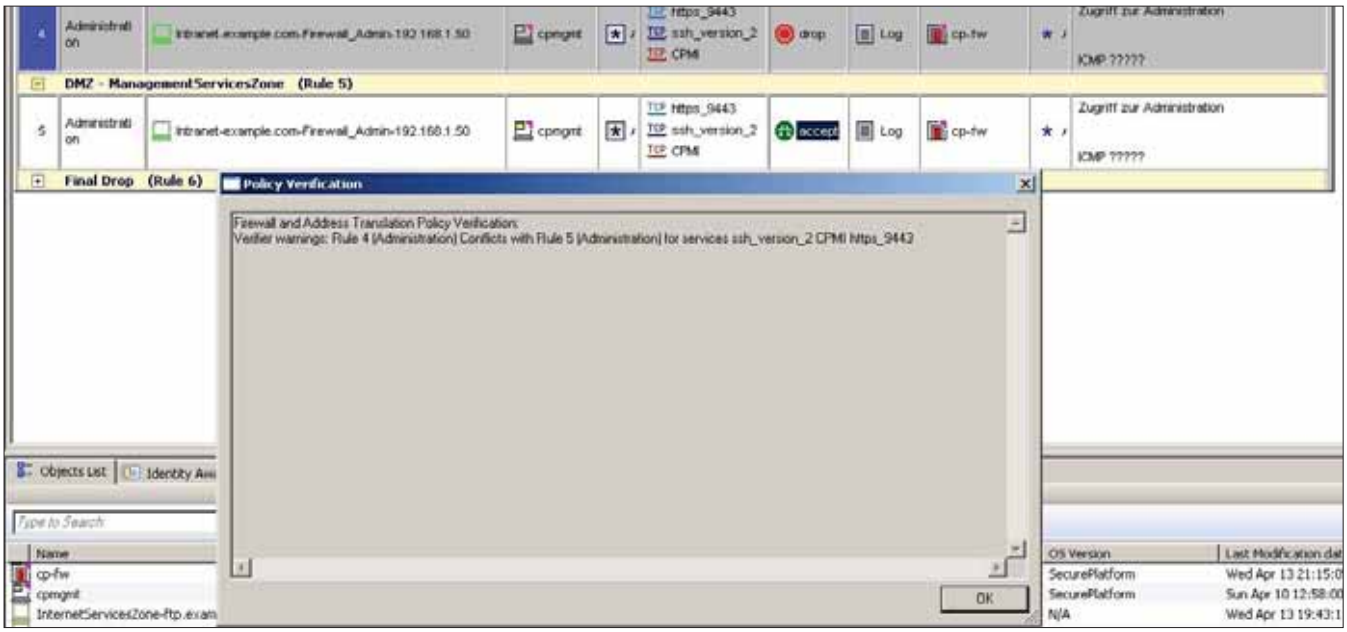


Abbildung 22. *„Policy Verification“ - Warning*

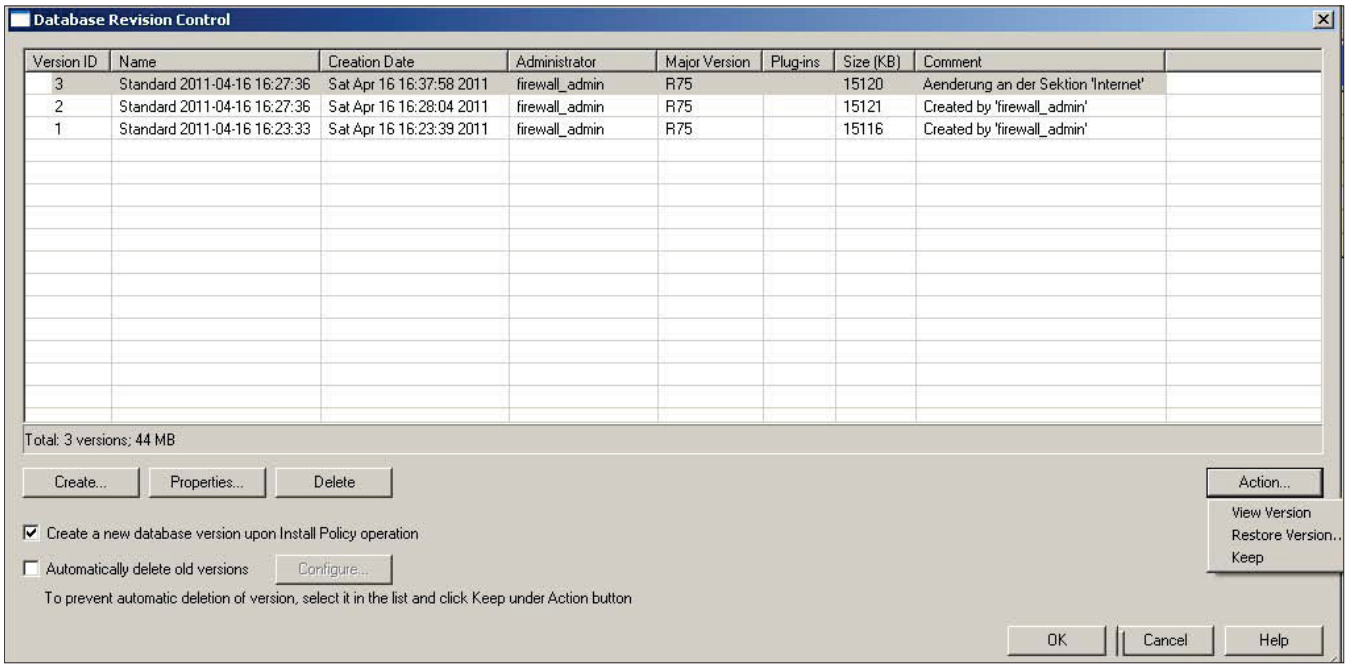


Abbildung 23. *Database Revision Control*

wissen Schutz bieten soll. *„Source->any, Destination->cp-fw, Service->any, Action->Drop"* (Abbildung11).

Final Drop

Die zweite Sektion bzw. Regel trägt den Namen „Final-Drop", und verwirft alle Pakete, die das Regelwerk komplett durchlaufen haben und für die es am Ende keine Übereinstimmung in dem Regelwerk gab. Diese Regel fügen wir am Ende (also aktuell als Nr. 2, hinter die „Stealth Rule) ein. *„Source->any, Destination->any, Service->any, Action->Drop"* (Abbildung12). Das Check Point Security Gateway besitzt zwar, durch die bereits erwähnten Implied Rules, eine derartige „Final-Drop"-Regel (Implicit Drop Rule), allerdings werden für diese **keine** Logeinträge erstellt, was aber für das Erkennen von möglichen Angriffen und/oder für das Debugging ungemein wichtig ist.

Security Management

Da durch die „Stealth Rule" sämtliche Anfragen an das Gateway selbst verworfen werden, muss als nächstes dafür gesorgt werden, dass die Möglichkeit der Administration per https_9443 und SSH besteht. Dazu wird die nächste Sektion „Firewall-Management" **über** der Sektion „Stealth-Rule" mit *„Rechte Maustaste auf die Sektion „Stealth Rule" -> Add Section Title -> Above*" erstellt. Unter dieser neuen Sektion wiederum wird eine Regel erstellt, die den Zugriff von der IP 192.168.1.50 für die Administration des Security Gateway erlaubt.*„Source->192.168.1.50, Destination->cp-fw, Service->https_9443/ssh_version2, Action->Accept"* (Abbildung13).

Zwingend notwendig für die Administration ist natürlich ebenfalls der Zugriff auf das zentrale Management, welches in einer eigenen DMZ steht. Um diesen Zugriff sicherzustellen, wird in die, unter der Stealth-Rule Sektion, liegenden Sektion mit der Bezeichnung „DMZ – ManagementServicesZone" eine Regel angelegt, welche den Zugriff von 192.168.1.51 auf das Management für die Ports https_9443, ssh_version2 und CPMI_18190 (Check Point Management Interface) erlaubt. *„Source->192.168.1.51, Destination->cpmgmt, Service->https_9443,ssh_version2,CPMI, Action->Accept*" (Abbildung14)

ICMP

Als nächstes wenden wir uns dem Thema ICMP zu. Da weder ein allgemeines Verbieten noch ein allgemeines Freigeben von ICMP sehr sinnvoll ist, wird die nächste Sektion „ICMP-Rules" **über** der Sektion „Stealth-Rule" erstellt. Hier wird nun eine Regel angelegt, welche „ICMP Destination Unreachable, ICMP Time Exceeded und ICMP Echo Request" für alle (any) freischaltet. *„Source->any, Destination->any, Service->dest-unreach/echo-request/time-exceeded, Action->Accept"* (Abbildung15).

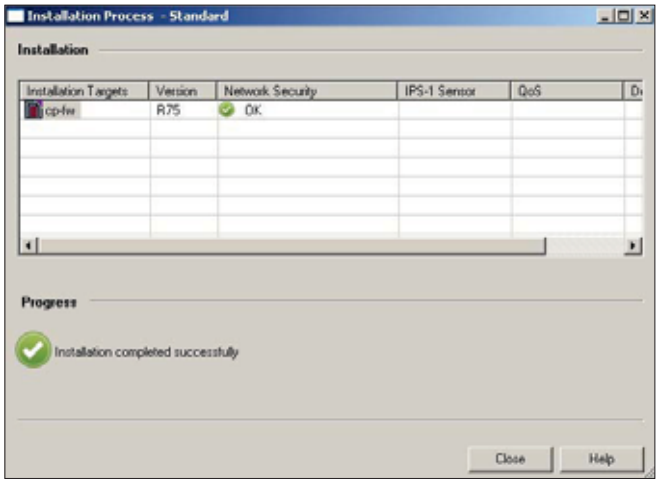


Abbildung 24. *Erfolgreiches „pushen" auf die Firewall-Nodes*

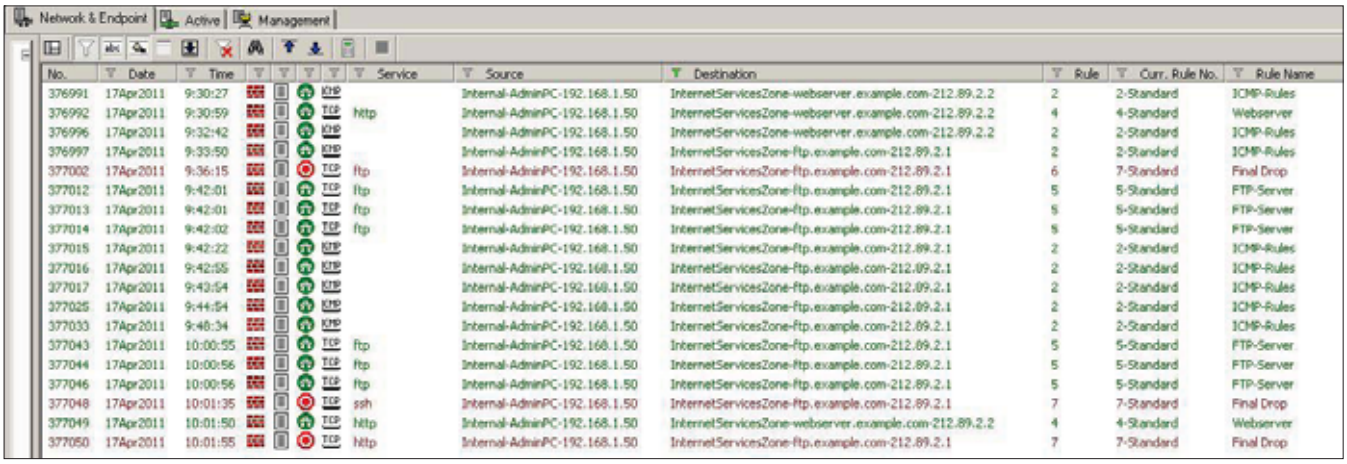


Abbildung 25. *Logkontrolle per SmartTracker*

Internet-Zugriff

Erlaubt für den Zugriff vom internen Netz in das Internet werden nur die Dienste http, https, ftp, smtp und pop3. Für diesen Zugriff wird auch erstmals das Objekt „UntrustedZone“ verwendet. Dieses Gruppen-Objekt „enthält“ alle Netze (any) mit Ausnahme, der in dem Gruppen-Objekt „Firewall-connectedNetworks“ hinterlegten Netze, in dem vorliegenden Fall also 192.168.1.0/24, 192.168.141.0/24, 212.89.2.0/24. *„Source->Internal-Network-192.168.1.0_24, Destination->UntrustedZone, Service->http,https,ftp.smtp,pop3, Action->Accept“* (Abbildung16). Damit nun das interne Netz auf das Internet zugreifen kann muss für das Netz ebenfalls eine NAT eingerichtet werden. Auf dem Check Point Security Gateway wird hierzu ein „Hide-Nat“ (bei Hide-Nat wird eine Port Address Translation durchgeführt) konfiguriert. *„Original Packet (Source->192.168.1.0/24, Destination->any, Service->any)/Translated Packet (Source->cp-fw(H), Destination->Original, Service->Original)”* (Abbildung17). Durch die zuvor konfigurierten Regeln, ist somit der Zugriff per http, https, ftp, smtp und pop3 ins Internet erlaubt und alle weiteren Zugriffe werden von dem Security Gateway geblockt und ins Log geschrieben.

Zu beachten ist bei der NAT-Konfiguration aber noch, dass durch das Setzen von „Destination->any“ unter „Original Packet“, auch für den Zugriff in Richtung DMZ-Bereiche ein NAT gemacht wird, was allerdings nicht gewollt ist. Also muss **über** der Hide-Nat-Regel zusätzlich eine weitere Regel erstellt werden, die dafür sorgt, dass zwischen den direkt verbunden Netzen **kein** NAT durchgeführt wird. *„Original Packet (Source->Firewall-connectedNetworks, Destination->Firewall-connectedNetworks, Service->any)/Translated Packet (Source->Original, Destination->Original, Service->Original)* (Abbildung18)

Web- und FTP-Server

Die letzten Regeln betreffen die Zugriffe auf Web- und FTP-Server, einmal aus dem Internet und zum anderen aus dem LAN. Hierzu werden unter der Sektion „DMZ – InternetServicesZone“, zwei Regeln erstellt. In der ersten Regel wird das Objekt „UntrustedZone“, diesmal allerdings als Source eingetragen und als Ziel der FTP-Server. *„Source->UntrustedZone, Destination->212.89.2.1, Service->ftp, Action->Accept“. D*ie zweite Regel bekommt als Ziel den Webserver mit den entsprechenden Ports http und https. *„Source->UntrustedZone, Destination->212.89.2.2, Service->http/https, Action->Accept“* (Abbildung19). Mit diesen Regeln ist sichergestellt, dass Web- und FTP-Server aus dem Internet erreichbar sind. Zugriffe aus dem internen Netz werden allerdings nach wie vor von der Firewall in der „Final Drop“-Regel geblockt, da mit den ersten beiden Regeln nur der Zugriff von nicht direkt verbunden Netzen (UntrustedZone) erlaubt wurde. Um dies zu ändern, werden die eben erstellten Regeln einfach mit *„Rechte Maustaste -> Copy“* kopiert und unter die ersten beiden Regeln mit *„Rechte Maustaste -> Paste -> Below“* eingefügt. Zuletzt wird dann einfach die Source „UntrustedZone“ gegen „Internal-Network-192.168.1.0_24„ ausgetauscht (Abbildung20). Somit ist nun ebenfalls sichergestellt, dass aus dem internen Netz auf Web- und FTP-Server zugegriffen werden kann.

Damit sieht das gesamte Regelwerk inklusive der erstellen Objekte wie in Abbildung21 dargestellt aus.

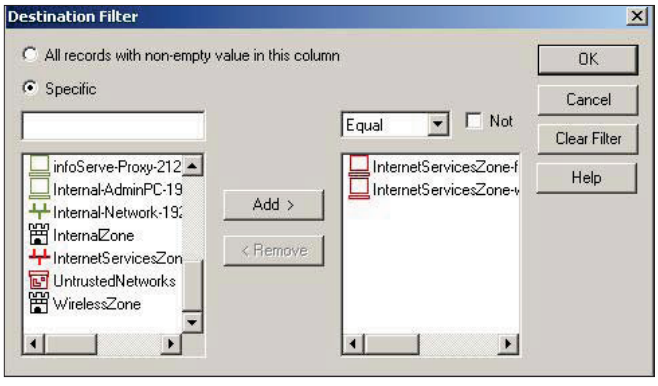


Abbildung 26. *Filter Konfiguration im SmartTracker*

Policy

Alle oben, per SmartDashboard, angelegten Objekte und Regeln existieren bisher ausschließlich auf dem Management, d.h. tatsächlich kennt das Security Gateway diese Regeln und Objekte aktuell noch gar nicht und wendet diese damit natürlich auch noch nicht an. Um das erstellte Firewall-Regelwerk nun auch auf dem Security Gateway zu aktivieren, muss man diese vom Management auf das Gateway „pushen".

Policy Verify

Vor der eigentlichen Installation besteht noch die Möglichkeit der Überprüfung des Regelwerks per *„Policy -> Verify*". Wird hier z. b. eine Überschneidung in den Regeln festgestellt, gibt es eine Warnung, welche Regeln und Dienste von der möglichen Fehlkonfiguration betroffen sind (Abbildung22). In dem gezeigten Beispiel wurde die an für sich gleiche Regel zweimal konfiguriert, mit dem Unterschied, dass in Regel 4 der Zugriff geblockt und in Regel 5 erlaubt würde. Diese Warnung würde allerdings ebenfalls erscheinen wenn man direkt ein Install Policy ausgeführt hätte.

Revision Control

Des Weiteren kann vor dem pushen der Regeln eine Revisions-Kontrolle per „*File -> Database Revision Control*" durchgeführt werden. Hier besteht die Möglichkeit eine Kopie der aktuellen Regeln und Objekte auf dem Management zu speichern bzw. eine frühere Version des Regelwerks zu betrachten und gegebenenfalls auch wiederherzustellen (Abbildung22). Die Revision Control kann ebenfalls direkt vor dem pushen erstellt werden und muss nicht jedes Mal manuell ausgeführt werden.

Policy Install

Um das pushen der Regeln nun durchzuführen, wählt man im SmartDasboard „*Policy -> Install*" aus. In dem nun erscheinenden Fenster stehen gegebenenfalls eine oder mehrere Gateways, auf welche das aktuelle Regelwerk gepusht werden kann und die „Revision Control" zur Auswahl. Mit einem Klick auf OK, startet die Übertragung der Regeln auf das Security Gateway und wird mit der Meldung „*Installation completed successfully*" (Abbildung24) bei erfolgreicher Übertragung abgeschlossen.

Im Internet

- *http://www.checkpoint.com* – die offizielle Check Point Website
- *http://downloads.checkpoint.com/dc/download.htm?ID=11550* – R75 Documentation Package
- *http://www.checkpoint.com/campaigns/nss-next-gen-firewall/index.html#* - NSS Labs Next Generation Firewall Test Report for Check Point

SmartTracker

Um nun die in das Log geschriebenen Einträge nachvollziehen zu können, steht das Tool „SmartTracker" zur Verfügung. Hier kann man alle im Regelwerk mit „*Track->Log*" versehenen Regeln, egal ob Accept oder Drop, verfolgen (Abbildung25). Wir zu erkennen, sieht man zum einen die üblichen Informationen, wie Port, Ziel- und Quell-IP, aber auch welche Regel den Zugriff erlaubt bzw. geblockt hat. Des Weiteren besteht die Möglichkeit, in den angezeigten Reitern eigene Filter zu hinterlegen (Rechte Maustaste -> Edit Filter), so dass man nur die wirklich gewünschten Informationen aus dem Log ziehen kann. (Abbildung26)

Fazit

Firewalls werden natürlich auch in Zukunft einen wichtigen Platz in der Netzwerk-Infrastruktur einnehmen und trotz aller möglichen Vorteile oder Vereinfachungen eines Produktes, gibt es immer noch genügend Fallen in die ein Security-Administrator tappen kann. Beispielsweise kann in ein Gruppen-Objekt schnell der falsche Host oder das falsche Netzwerk eingetragen werden und damit ungewollte Zugriffe auf Systeme frei geschaltet werden.

Auch wird die Komplexität weiterhin steigen und bereits heute kann eine („reine") Firewall, viele Anforderungen an die „Sicherheit" gestellt werden nicht mehr alleine erfüllen, was unweigerlich dazu führt das weitere Security-Komponenten integriert werden müssen. Dies wiederum stellt die Administratoren vor die Aufgabe, sich mit unterschiedlichen Methoden und verschiedenen Konfigurationsansätzen zu beschäftigen. Auch in diesem Punkt schafft Check Point mit Hilfe seines (zentralen) Managements, in dem die Software-Blades administriert werden können, gute Abhilfe. Darüber hinaus bietet das Management noch eine Menge weiterer kleiner Hilfen, die einem Administrator das Leben durchaus erleichtern können, wie z. b. die Möglichkeit mit „Where Used ..." auf ein Objekt um zu sehen in welchen Regeln bzw. Policies dieses Objekt verwendet wird. Nicht vergessen sollte man aber auch, dass im Umfeld von Check Point, das meiste einen stolzen Preis hat und natürlich auch immer eine entsprechende Lizenz gekauft werden muss. Doch trotz aller Vor- und Nachteile von den jeweiligen Produkten, bleiben am Ende die (Security)-Administratoren die wohl wichtigste „Komponente" und werden weiterhin verstärkt in der Pflicht sein, sich Gewissenhaft an Vorgaben zu halten und über zu konfigurierende Zugriffe genau nachzudenken, um es am Ende einem Angreifer nicht allzu leicht zu machen.

STEFAN SCHURTZ

Der Autor arbeitet bei einem saarländischen ISP im Bereich Netzwerk-Sicherheit und beschäftigt sich auch privat mit dieser Thematik

Kontakt mit dem Autor: sschurtz@t-online.de

Cyber-Angriff auf Comodo sorgt für Wirbel

Christian Heutger, PSW GROUP

Auf das IT-Sicherheitsunternehmen Comodo und damit auf eine tragende Säule der Internet-Sicherheitsinfrastruktur ist am 15. März 2011 die wahrscheinlich spektakulärste Cyber-Attacke des noch jungen Jahres erfolgt. Gründer und CEO Melih Abdulhayoglu verglich den Angriff, der Hackern aus dem Iran zugeschrieben wird, von der Vorgehensweise her gar mit dem „11. September".

IN DIESEM ARTIKEL ERFAHREN SIE...

- Wissenswertes über die Vorgehensweise der Angreifer
- Informationen über die betroffenen Websites und „gestohlenen" SSL-Zertifikate
- Die möglichen politischen Zusammenhänge

WAS SIE VORHER WISSEN SOLLTEN...

- Um die Hintergründe der Attacke zu verstehen, ist es notwendig sich noch einmal die Funktion beziehungsweise Stellung von Comodo im Bereich der globalen Internet-Sicherheit ins Gedächtnis zu rufen. Das Unternehmen zählt neben VeriSign zu einer der wenigen etablierten so genannten Certificate Authorities (CA), die SSL-Zertifikate signieren und somit eine der zentralen Säulen der Sicherheitsinfrastruktur im Internet verwalten. In jedem Web-Browser ist ein sogenanntes Root-Zertifikat platziert, das dem Browser mitteilt, dass Comodo-Zertifikate vertrauenswürdig sind.

Auch wenn sich der Schaden in Grenzen hielt, offenbarte die Attacke auf Comodo große Schwachstellen und könnte sogar eine politische Dimension haben. Nicht von ungefähr wird sie in Sicherheitskreisen bereits „Comodgate" genannt. Erste Lehren aus der Attacke wurden bereits gezogen: So sind die Sicherheitsvorkehrungen bei Comodo verschärft worden.

Das Vorgehen: Attacke via Reseller

Angegriffen wurde Comodo allerdings nicht direkt. Gehackt wurde vielmehr der Account eines als Registry Authority (RA) eingestuften, italienischen Resellers des Unternehmens, dessen Aufgabe es in dieser Funktion ist, die Echtheit der in Zertifikatsanträgen aufgeführten Informationen zu überprüfen und diese Anträge dann weitgehend automatisiert von Comodo als Zertifizierungsstelle signieren zu lassen.

Der Hacker verschaffte sich dabei Zugang zu einem Nutzer-Account des Resellers und erzeugte mit diesem eine eigene, neue User-ID – inklusive neuem Nutzernamen und Passwort. Er war sehr gut vorbereitet und schien eine Liste mit seinen Ziel-Domains abzuarbeiten. Für diese orderte er Zertifikate und generierte die hierfür erforderlichen CSRs (Certificate Signing Requests). Dabei handelt es sich um Anträge auf die Signierung eines öffentlichen Schlüssels durch eine Certificate Authority, in diesem Fall Comodo.

Aber von Anfang an: Der Hacker war offenbar zunächst in den Web-Server des italienischen Comodo-Resellers eingedrungen, wo er eine .NET-Bibliothek vorfand, mit der der Reseller die CSRs bei unter anderem Comodo für die Ausstellung eines SSL-Zertifikats einreicht. Durch Dekompilieren der Bibliothek ist er schließlich an die Zugangsdaten für den Comodo-Reseller-Account gelangt, die hart-codiert in dieser hinterlegt waren. Über die vorhandene API-Schnittstelle gelang es ihm dann die Anträge für die entsprechenden Domains einzureichen, die das eigentliche Ziel der Attacke waren.

Als systemimmanente Schwachstelle erwies sich bei dem Hacker-Angriff die unlängst kontrovers diskutierte Praxis der so genannten Selbstvalidierung. Heißt: Die Registry Authorities (RAs) – in diesem Fall der als solche eingestufte Reseller – können sich meist automatisiert selbst die Echtheit der von ihnen validierten

SSL-Zertifikate bestätigen. Die Attacke hätte somit aller Wahrscheinlichkeit nach auch über andere RAs erfolgreich ausgeführt werden können.

Ausmaß des Hacks

Durch den Angriff wurden unter Umgehung der üblichen Validierungsverfahren nach aktuellem Kenntnisstand für sieben bekannte Websites – darunter die von Google Mail, Yahoo, Skype, Windows Live und Mozilla – zusätzlich neun unvalidierte SSL-Zertifikate zu den bereits bestehenden ausgestellt.

Betroffen waren folgende Domains und Zertifikate:

- Domain: *mail.google.com*
  Serial: 047ECBE9FCA55F7BD09EAE36E10CAE1E
- Domain: *www.google.com*
  Serial: 00F5C86AF36162F13A64F54F6DC9587C06
- Domain: *login.yahoo.com*
  Serial: 00D7558FDAF5F1105BB213282B707729A3
- Domain: *login.yahoo.com*
  Serial: 392A434F0E07DF1F8AA305DE34E0C229
- Domain: *login.yahoo.com*
  Serial: 3E75CED46B693021218830AE86A82A71
- Domain: *login.skype.com*
  Serial: 00E9028B9578E415DC1A710A2B88154447
- Domain: *addons.mozilla.org*
  Serial: 009239D5348F40D1695A745470E1F23F43
- Domain: *login.live.com*
  Serial: 00B0B7133ED096F9B56FAE91C874BD3AC0
- Domain: *global trustee*
  Serial: 00D8F35F4EB7872B2DAB0692E315382FB0

Den Angaben von Comodo zufolge wurde allerdings keines der SSL-Zertifikate kompromittiert. Benutzt wurde aber eines der gefälschten SSL-Zertifikate für Yahoo – offenbar für einen Test, den der Angreifer durchgeführt hatte. Aus den Hardware-Security-Modulen (HSM) sind laut Comodo aber keinerlei Schlüssel entwendet, Algorithmen geknackt oder Zertifikate nachgebaut worden.

Was wäre wenn …

Wäre die Hacker-Attacke – wie vom Angreifer beabsichtigt – erfolgreich verlaufen, hätte er zumindest den seine Region betreffenden Teil der über die anvisierten Domains laufenden Kommunikation als „man in the middle“ über Skype, Google Mail & Co. „belauschen“ können. Denn mit den „gestohlenen“ SSL-Zertifikaten wäre es ihm ohne weiteres möglich gewesen, eigene manipulierte beziehungsweise nachgeahmte Websites jedem Browser gegenüber als Originale auszugeben. Eine solche Überwachung, von der der Nutzer aufgrund des scheinbar gültigen SSL-Zertifikats nichts geahnt hätte, hätte aber vorausgesetzt, dass der Hacker zugleich Zugriff auf DNS-Server hat. Denn:

+ Jedem Domainnamen (etwa psw.net) ist eine feste IP-Adresse zugeordnet.
+ Diese für den Aufruf einer Website notwendige Information fragt der Browser bei einem der weltweit verteilten DNS-Server – in der Regel einem in der entsprechenden Region des Nutzers – an.
+ Damit der Nutzer nicht auf der echten, sondern auf der manipulierten, nachgeahmten Website des Angreifers landet, muss ihn sein Browser auf eine – eigentlich falsche – IP-Adresse weiterleiten. Dies ist einem Angreifer nur mit Hilfe von DNS-Manipulationen möglich.

Über addons.mozilla.org hätte der Angreifer aber sogar Schad-Software auf die Rechner von Firefox-Nutzern einschleusen oder gar die Installation von Addons blockieren können, die das Umgehen von Zensurbemühungen eines Staates wie dem Iran ermöglichen. Zwar sind Web-Browser generell durch Prüfmechanismen wie OCSP und CRL in der Lage, gefälschte Zertifikate zu erkennen – ein Angreifer, der ein solches nutzt, könnte als „man in the middle“ aber auch die Antworten auf diese Prüfanfragen des Browsers wirksam unterbinden.

Die Konsequenzen: Verschärfung der Sicherheitsvorkehrungen

Der Angriff wurde binnen Stunden aufgedeckt und die manipulierten SSL-Zertifikate gelöscht. Außerdem wurden umgehend nach Bekanntwerden des Vorfalls die betroffenen Website-Betreiber, die größten Browser-Hersteller sowie auch die zuständigen Regierungsbehörden informiert. Nur kurze Zeit nach Bekanntwerden des Cyber-Angriffs hat Comodo reagiert und den Zugang zu seinen Systemen eingeschränkt sowie die standardisierte Validierung von Zertifikaten überarbeitet. Die Authentifizierungsplattform von Comodo wurde außerdem um neue Kontrollmechanismen erweitert. So wird fortan nicht nur schärfer validiert, sondern es kommt auch eine generelle Domainvalidierung zum Einsatz. Teilweise erfolgt die Ausstellung von SSL-Zertifikaten auf Seiten von Comodo ab sofort durch manuelle Freigabe. Auf diesem Wege schließt Comodo aus, dass sich ein derart gelagerter Angriff unter Nutzung der bisherigen Automatismen bei Comodo wiederholen kann.

Der Hacker nutzte den kompromittierten Reseller-Account übrigens noch, als die Attacke aufgedeckt wurde. Der Account wurde daraufhin deaktiviert, so dass der Angreifer keine Möglichkeit mehr hatte, weitere SSL-Zertifikate zu erstellen.

Weitere Attacken

Am 26. März 2011 kam es bei einem zweiten Reseller zu einer weiteren Attacke, die scheinbar auf denselben

Angreifer zurückzuführen war. Noch eine Attacke ereignete sich bei einem dritten Reseller von Comodo. Sie entpuppte sich nach genauen Nachforschungen allerdings als Login-Fehler seitens eines Nutzers.

Doch nicht nur Comodo stand in letzter Zeit unter Beschuss. Auch andere Sicherheitsanbieter sahen sich mit Attacken konfrontiert. Mitte April 2011 wurde die Website der US-Sicherheitsfirma Barracuda Networks gehackt. Dabei wurden Kunden- und Mitarbeiterdaten gestohlen. Der Angreifer bediente sich bei der Attacke einer SQL-Injenction-Lücke in einem PHP-Script auf dem Webserver des Unternehmens.

Bereits wenige Tage vor der Attacke auf den zweiten Comodo-Reseller war außerdem ein Angriff auf den Verschlüsselungsspezialisten RSA bekannt geworden. Auch hier wurden Daten von Unternehmensservern entwendet – darunter Daten für die SecurID-Tokens des Anbieters, die bei über 40 Millionen Unternehmen weltweit im Einsatz sind. Ebenfalls im Visier stand das US-amerikanische IT-Sicherheitsunternehmen HBGary. Es war bei der Gruppierung Anonymous in Ungnade gefallen und von deren Anhängern Anfang Februar gehackt worden. Der Angriff, bei dem HBGary über 60.000 E-Mails gestohlen wurden, erfolgte – ebenfalls per SQL-Injenction – über das Content Management System der Website des Unternehmens.

Politische Dimension: Hack im Auftrag der iranischen Regierung?

Die Attacke ging von einer Reihe von verschiedenen IP-Adressen aus, überwiegend konnten diese jedoch dem Iran zugeordnet werden – so unter anderem die IP-Adresse 212.95.136.18.

Stadt: Teheran
Land: Islamische Republik Iran
ISP: Pishgaman TOSE Ertebatat Tehran Network

Weitere Untersuchungen ergaben, dass eines der vom Hacker erstellten Zertifikate mit einer weiteren IP-Adresse – ebenfalls dem IP-Adress-Blocks eines iranischen Providers angehörig – korrespondierte. Auch die durch den Hack betroffenen Domains scheinen in diesem Zusammenhang eine deutliche Sprache zu sprechen, handelt es sich doch um die von politischen Dissidenten am häufigsten genutzten Websites. Dass totalitäre Regime wie der Iran ein Interesse an der Überwachung eben solcher Seiten hat, steht außer Frage.

Der Comodo-Hack fällt außerdem in eine gerade für den arabischen Raum politisch brisante Zeit. Unruhen in Form von Protesten seitens Oppositioneller und Demokratie-Bewegungen – auch als „arabische Revolution“ bezeichnet – bestimmen derzeit das Bild in Nordafrika und auf der arabischen Halbinsel. Das Internet und gerade Social Networks haben sich hier zu einem beliebten Organisationstool für Proteste entwickelt. Außerdem sind Attacken seitens Regierungen gegen Social Networks kein neues Phänomen. Zu Beginn der Proteste in 2009 hat die so genannte „Iranian Cyber Army“ den Zugang zu Twitter verhindert. In Ägypten und Libyen wurde zeitweise immer wieder sogar das komplette Internet gesperrt. Tunesische Regierungsbehörden initiierten gar eine JavaScript-Attacke gegen Social Networks.

Interessant ist vor allem, dass der Angreifer mit unter anderem Google Mail, Yahoo Mail, Skype und Windows Live einen Fokus auf die Internet-Kommunikation gelegt hat. Das spricht ganz deutlich für eine politisch motivierte – womöglich von einer Regierung initiierten – Attacke. Cyber-Kriminelle hingegen zielen vornehmlich auf finanzrelevante Online-Infrastrukturen ab. Außerdem hätte der Angreifer die von ihm erzeugten Zertifikate – wie dargelegt – nur nutzen können, wenn er Zugriff auf Teile der DNS-Infrastruktur hat. Besonders auffällig war die beinahe schon klinische Sorgfalt, die der Hacker bei seiner Attacke hat walten lassen.

Online-Bekenntnis eines 21-Jährigen

Zur Attacke bekannt hat sich in einem Online-Manifest ein 21-Jähriger, der sich selbst als „ComodoHacker“ bezeichnet. Er stammt offenbar aus dem Iran und zeigt in seinen Ausführungen einen gewissen Hang zum Patriotismus. Der „ComodoHacker“ will den Hack allein ausgeführt haben, was bezweifelt werden darf. Vielmehr liegt in Anbetracht der Sachlage eine so genannte „state-driven“-Attacke nahe. Gegen eine Verwicklung der iranischen Regierung in die Vorgänge spricht auch nicht, dass der „ComodoHacker“ nach eigenen Angaben in keiner Beziehung zur bereits in Erscheinung getretenen „Iranian Cyber Army“ steht.

CHRISTIAN HEUTGER

Der Autor ist Geschäftsführer der PSW GROUP GmbH & Co. KG und verfügt über mehr als elf Jahre Erfahrung in der Branche für SSL-Zertifikate. Sein Wissen über IT-Sicherheit vermittelt er als Lehrbeauftragter für den DV-Bereich am Fachbereich Wirtschaft der Hochschule Fulda und im Rahmen seiner nebenberuflichen Tätigkeit als Informatiklehrer am Marianum Fulda.

ISO/IEC 27001 für Informationssicherheit: „Business Needs auf die IT herunter brechen“

Laut InfoWatch-Statistik gehen pro Tag weltweit bis zu 3 Millionen Personendatensätze verloren. Davon rund 75 Prozent unbeabsichtigt, ohne kriminelle Energie. Vor diesem Hintergrund entscheiden sich immer mehr Unternehmen für eine strukturierte Absicherung mittels Prozessmanagement nach ISO/IEC 27001: Mehr als 12.000 Unternehmen in 80 Ländern sind mittlerweile nach dem Information-Security-Standard ISO 27001 zertifiziert. Pro Jahr kommen rund 1.000 dazu, auch aus dem KMU-Bereich. Erich Scheiber, Geschäftsführer der weltweit tätigen Zertifizierungsorganisation CIS, beschreibt im Interview einen „hohen internen Schutzbedarf“ und gibt Tipps zur ISO-27001-Implementierung.

Herr Scheiber, was sind häufige Versäumnisse von Unternehmen im Bereich Informationssicherheit?
Auf den Punkt gebracht: Die große Techniklastigkeit mit zu wenig Augenmerk auf organisatorische Aspekte. Im Annual Global Security Survey von Ernst & Young wurde gewarnt, dass bis zu 80 Prozent der Security-Budgets in technische Maßnahmen fließen und zu wenig in die Sicherheitsorganisation investiert wird. Auch das Messen und Kontrollieren der Effizienz von Security-Maßnahmen wird häufig vernachlässigt. Klare Definitionen von Anforderungen und Risiken fehlen oft.

Warum entscheiden sich Unternehmen quer durch alle Branchen für eine Zertifizierung nach dem Security-Standard ISO/IEC 27001?
„Lokale wie internationale Studien belegen einen hohen internen Schutzbedarf. In der betrieblichen Praxis ist deshalb ein Trend zu beobachten: weg von Einzel-Security-Maßnahmen hin zu strategischen und ganzheitlichen Konzepten. ISO 27001 ist weltweit das einzige Regelwerk, welches eine Zertifizierung der implementierten Informationssicherheit ermöglicht. Das Zertifikat bringt handfeste Vorteile im Wettbewerb.

Welche Inhalte deckt ISO 27001 ab?
Der Security-Standard umfasst neben einem strukturierten Vorgehen bei IT-sicherheitstechnischen Fragen je nach Anforderung auch Organisation, Awareness oder physische Sicherheit wie Gebäude- und Brandschutz. Die Umsetzung erfolgt mittels Risikoanalyse, Daten-Klassifizierung, Policies und Maßnahmenkon-

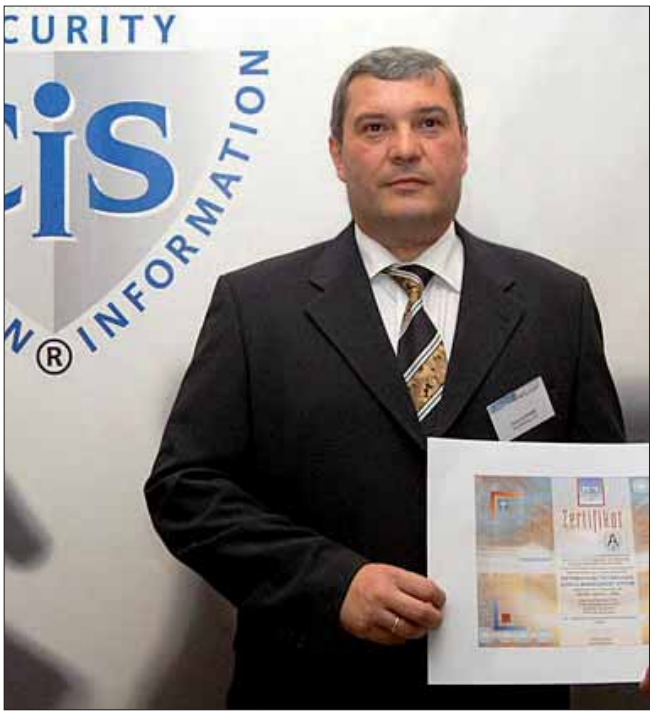


Abbildung 1. ***CIS-Geschäftsführer Erich Scheiber:*** *„Grund für das hohe Ansehen von CIS-Zertifikaten ist die Qualität der Akkreditierung durch das österreichische Wirtschaftsministerium. Dadurch entsprechen CIS-Zertifikate staatlichen Dokumenten und gelten international bei Behörden und Kunden sowie auch vor Gericht als geprüfter Sorgfaltsnachweis.“*

trollen nach dem Prozessmodell Plan-Do-Check-Act. Damit bietet ISO 27001 ein systematisches Framework zum Schutz von Informationen. Standardisierung schafft verbesserte Prozesse und dadurch auch eine verbesserte Kommunikation in Bezug auf Datenschutz und Informationssicherheit im Unternehmen.

Welche Branchen sind Vorreiter?

Produktionsunternehmen sind sehr aktiv, weil sie die Kultur von Prozessmanagement und Auditing aus dem Qualitäts- oder Umweltmanagement kennen. Im Dienstleistungssektor sind es vor allem Software- und IT-Service-Anbieter, Banken, Versicherungen, Energieversorger, Gesundheitseinrichtungen oder öffentliche Institutionen. Aber auch Consulter und kleinere Unternehmen aus verschiedenen Branchen. ISO 27001 ist technologie-, branchen- und größenunabhängig und daher auch gut für die Anwendung in KMU geeignet.

Welche Tipps geben Sie zur Implementierung von Informationssicherheit?

Man sollte sich immer zuerst die Frage stellen: Wie viel ist zu investieren, um ein wirtschaftlich vernünftiges Maß an Informationssicherheit zu erreichen? ISO 27001 fordert kein unfinanzierbares Optimum, sondern steht für wirtschaftlich rentable Sicherheit auf dem höchstmöglichen Niveau.

Was sind typisch unterschätzte Bedrohungen?

Schwachpunkte, die wir in der Praxis finden, betreffen zum Beispiel die physischen Zutrittskontrollen. Es nützt die beste Firewall nichts, wenn Fremde in der Mittagspause zu den Arbeitsplätzen gelangen. Oder wenn bei einem Ausfall des Zutrittssystems ohne Notfallplan Türen freigeschaltet werden. Auch bei der Notstromversorgung gibt es wichtige Details: In einem großen Rechenzentrum war die Notstromversorgung der Server zwar sichergestellt, aber nicht jene der Klimatisierung – die Folge hätte ein Systemausfall durch überhitzte Rechner sein können. Ebenfalls werden Netzwerke nach außen meist gut gesichert, aber unzureichend gegen Angriffe aus den eigenen Reihen.

Welche Aspekte sind in der Security-Organisation erfolgsentscheidend?

Bei der Einführung eines Managementsystems von Informationssicherheit, kurz: ISMS, steht die Definition von messbaren Zielen an erster Stelle. Sonst können die besten Bestrebungen im Sande verlaufen. Eine gute Hilfestellung bietet die Zertifizierung nach ISO 27001 als Endziel – auch als Motivationsfaktor für die Mitarbeiter. Ebenfalls bewährt sich die Einbindung aller Unternehmensbereiche in der Implementierungsphase wie Rechtsabteilung, kaufmännische Bereiche, Marketing und Vertrieb. Denn das ISMS muss letztendlich von allen Mitarbeitern gelebt werden. Wird dieser Punkt zu wenig beachtet, kann es durch Kompetenzverschiebungen zu Hindernissen kommen: Wenn gute Fachleute von Kollegen blockiert werden leidet das ganze System darunter.

Welche Strategie empfehlen Sie für die Risikoanalyse?

ISO 27001 sieht Risikomanagement verpflichtend vor. Bewertet werden dabei Eintrittswahrscheinlichkeiten von Vorfällen, potentielle Schäden und der finanziel-

Abbildung 2. ***Von der Implementierung zum Zertifikat:*** *Der Ablauf eines Zertifizierungsprojektes für ein Informationssicherheitsmanagementsystem nach ISO 27001 (ISMS) teilt sich in drei Phasen. Dieser Ablauf gilt auch für Integrierte Managementsysteme in Kombination mit ISO 20000 für IT-Service-Management oder ISO 9001 für Qualitätsmanagement.*

Abbildung 3. ***Risikomanagement nach ISO 27001*** *In der Zertifizierungsnorm ISO 27001 für Informationssicherheit wird Risikomanagement explizit gefordert, um die IT- und Ressourcenverfügbarkeit sicherzustellen. Bei der Umsetzung hilft der nicht-zertifizierbare RM-Leitfaden ISO 27005 mit Beispielen und detaillierten Ausführungen.*

le Aufwand von Security-Maßnahmen. Die Business-Needs sollten dabei auf die IT herunter gebrochen werden und nicht umgekehrt. Ausgehend von den Geschäftsprozessen wird evaluiert, welche Security-Maßnahmen erforderlich sind, um diese Aufrecht zu erhalten, wobei die Kosten-Nutzen-Relation wesentlich ist. Um die praktische Umsetzung zu erleichtern, bietet sich die Nutzung der Subnorm ISO 27005 mit seinen Beispielen und Modellen an.

Mit welchen Motiven implementieren Unternehmen Security-Systeme nach ISO 27001?

Ein nach innen gerichtetes Motiv betrifft die ständige Optimierung der betrieblichen Sicherheit. Durch den in der Norm geforderten Verbesserungsprozess nach dem Modell Plan-Do-Check-Act wird das System laufend an geänderte Anforderungen angepasst. Evident ist auch der Wettbewerbsdruck. Konzerne wie Automobilhersteller, Mineralölgesellschaften oder IKT-Unternehmen verlangen von Zulieferern häufig eine Zertifizierung nach ISO 27001 als Nachweis für lückenlose Informationssicherheit. Auch bei Ausschreibungen gilt ein ISO-27001-Zertifikat als schlagendes Wettbewerbskriterium. Zudem gilt eine ISO-Zertifizierung als geprüfter Sorgfaltsnachweis im juristischen Sinne und hat Gültigkeit vor Gericht. Ein Zertifikat nach ISO 27001 minimiert das Haftungsrisiko von Unternehmen und Führungskräften.

Erich Scheiber ist Geschäftsführer der Zertifizierungsorganisation CIS - Certification & Information Security Services GmbH mit Sitz in Wien. Mit der Spezialisierung auf Informationssicherheit nach ISO/IEC 27001 und IT-Service-Management nach ISO/IEC 20000 ist CIS als Global Player in rund 30 Nationen präsent. www.cis-cert.com

Security und Quality als Integriertes Managementsystem

Informationssicherheit nach ISO 27001 lässt sich nahtlos in das Qualitätsmanagement nach ISO 9001 integrieren oder zeitgleich einführen. Durch Kombinationsaudits, gemeinsame Reviews und einheitliche Dokumentation sparen Unternehmen 20 bis 30 Prozent Aufwand.

In der betrieblichen Praxis geht der Trend in Richtung Integration von Managementsystemen: Die ISO-Standards für Informationssicherheit (ISO 27001), IT Service Management (ISO 20000), Qualität (ISO 9001) und Umwelt (ISO 14000) sind in ihrem Aufbau und Prozessansatz ähnlich und stellen dieselben Anforderungen wie etwa in der Verantwortlichkeit des oberen Managements, Zielsetzung der ständigen Verbesserung oder in der Systematik der Dokumentation.

20 bis 30 Prozent Synergien

„Eine Integration ermöglicht die Nutzung enormer Synergien. Im laufenden Betrieb spart man 20 bis 30 Prozent Aufwand für Systemoptimierung, Reviews und Audits“, erklärt Erich Scheiber, Geschäftsführer der weltweit tätigen Zertifizierungsorganisation CIS mit Sitz in Wien. Darüber hinaus sei der integrative Ansatz auch für Unternehmen hilfreich, die noch kein Prozessmanagement im Einsatz haben und mehrere Managementthemen wie Security und Quality zeitgleich implementieren wollen.

8 Monate für 2 Standards

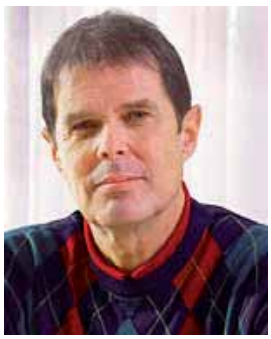


Abbildung 1. *Peter Soudat, CIS-Auditor:* ***„Informationssicherheit nach ISO 27001 schützt das Potenzial des Unternehmens, Qualitätsmanagement nach ISO 9001 bringt es hervor.”***

Eine reibungslose Integration von Informationssicherheit (IS) und Qualitätsmanagement (QM) zeigt das Beispiel der EDVG Elektronische Datenverarbeitung GmbH in Wien, die sowohl ISO 9001 als auch ISO 27001 in nur acht Monaten betriebsbereit implementierte und in weiteren drei Monaten zur Zertifizierungsreife brachte. Der etablierte IT-Dienstleister bedient Großkunden mit sensiblen Personendaten wie den Österreichischen Gewerkschaftsbund oder die Arbeiterkammer. „ISO 9001 und ISO 27001 haben identische Elemente. Reviews, Gremienmeetings und Audits werden bei uns integriert durchgeführt“, erklärt EDVG-Qualitätsmanager Gustav Jung.

Security & Quality: ein Ziel, ein Weg

Gemäß dem integrativen Ansatz wurde das Projektteam mit drei Personen für Projektleitung, QM und IS besetzt. „Wir hatten zwei Hauptzielrichtungen: einerseits alle Abläufe ISO-konform umzusetzen, andererseits diese in den Köpfen der Mitarbeiter zu verankern“, resümiert EDVG-Projektleiter Alfons Ankerl. Schon bei der Definition der Unternehmensziele zeigten sich Vorteile: „Für uns war es günstig, das IS-System an einem QM-Unternehmensziel – ein kompetenter Serviceprovider für unsere Kunden zu sein – auszurichten. Damit positioniert sich die Informationssicherheit als zentraler Business Enabler“, so Rudolf Kanov, Information Security Manager der EDVG.

Mapping Tabelle

Stellt man ISO 27001 und ISO 9001 gegenüber, so basieren beide auf der ständigen Verbesserung nach Plan-Do-Check-Act und korrespondieren in ihrer Struktur wie die Mapping Tabelle in Annex C der ISO 27001 zeigt: Auf Prozess-Ansatz und Scoping folgen in beiden Regelwerken Definitionen, Systemanforderungen, Dokumentation und Verantwortlichkeit des Managements. In beiden Fällen schließt die Struktur mit internen Audits, Management Review und Systemverbesserung. An diesen Schnittstellen ergeben sich inhaltliche Synergien. So fordert ISO 9001 die Kontrolle von fehlerhaften Produkten,

Abbildung 2. *Gustav Jung, Qualitätsmanager, EDVG:* ***„Die ISO-27001-Zertifizierung steigert den Business Value unserer Leistungen.“***

Abbildung 3. *Als Zertifizierungsorganisation für ISO 27001 und ISO 20000 bietet CIS effiziente Kombinationsaudits für Integrierte Managementsysteme. CIS mit Hauptsitz in Wien ist weltweit in rund 30 Nationen präsent. Aufgrund der Kooperation mit der ebenfalls international tätigen Zertifizierungsorganisation qualityaustria können kombinierte Auditorenteams weltweit in Unternehmen eingesetzt werden.*

was der 27001-Forderung nach Incident Management zur Behebung von IT-Störungen entspricht.

Unterschiede als Stärke

„Auch die Unterschiede zwischen den Standards stellen sich als sinnvolle Ergänzungen dar", erklärt CIS-Auditor Peter Soudat. „Informationssicherheit schützt das Potenzial des Unternehmens, Qualitätsmanagement bringt es hervor." So fordert ISO 9001 die Definition von Unternehmenszielen, Kundenorientierung und messbare Zielerreichung. Diese drei Punkte stehen bei ISO 27001 nicht im Vordergrund. Dafür legt diese Gewicht auf Risikomanagement zur Wahrung der Business Continuity. Demgegenüber bezieht ISO 9001 Risiken nur allgemein auf das Umfeld.

Pas-de-Deux bei Policies

Das Qualitätsmanagement fungiert bei der EDVG als Dachsystem, während Informationssicherheit die IS-Ziele spezifiziert. Ähnlich wurde bei der Erstellung der Policies verfahren. Die Struktur der QM-Policy dient als Grundgerüst für die IS-Policy. Auch in der Dokumentation schließt sich der Kreis: Gemäß ISO 9001 regeln Richtlinien, wo welche Dokumente durch wen abzulegen und wie lange aufzubewahren sind. Mittels Klassifizierung nach ISO 27001 konnte die EDVG diese Anforderungen vertiefen. Für „Informationsdrehscheiben" wie Arbeitsplatz, E-Mail, Fax oder Telefon wurden Policies für höchsten Schutz erarbeitet. „Da die EDVG Millionen von Personendaten verwaltet, ist Datensicherheit geschäftskritisch", betont Gustav Jung. „Informationssicherheit nach ISO 27001 steigert den Business Value unserer Leistungen."

Finale mit ISO 20000

Insgesamt war das EDVG-Team so zufrieden mit dem Zusammenspiel von Qualitätsmanagement und Informationssicherheit, dass in nur weiteren sieben Monaten auch ISO 20000 für IT-Service-Management integriert und zertifiziert wurde. Gustav Jung: „Im Nachhinein betrachtet hätten wir ISO 20000 auch in einem Zuge mit ISO 9001 und 27001 implementieren können. Durch den ähnlichen Aufbau ist ein integrativer Ansatz fast vorgegeben. Diese Synergien sollten Unternehmen nutzen."

„Bauanleitung“ für Informationssicherheit: ISO 27003

CIS-Auditor Herfried Geyer

Zertifizierte Informationssicherheit nach dem Security-Standard ISO 27001 kommt vor allem in Großunternehmen zum Einsatz. Mit dem Implementierungsleitfaden ISO 27003 gelingt es auch KMU, ein Managementsystem nach internationalem Niveau aufzubauen: „Do it Yourself…“

Mit der Subnorm ISO/IEC 27003 liegt ein praxisnaher Implementierungsleitfaden vor: „Eine Chance auch für kleinere Unternehmen, Informationssicherheit bis zur Zertifizierungsreife Schritt für Schritt einzuführen“, betont Herfried Geyer, Auditor der weltweit tätigen Zertifizierungsorganisation CIS mit Sitz in Wien. Während der Zertifizierungsstandard ISO/IEC 27001 mit seinen Managementspezifikationen die Frage nach dem „Was“ beantwortet, behandelt ISO/IEC 27003 mit Checklisten und Beispielen die Frage nach dem „Wie“. Ihr Inhalt erstreckt sich auf die Einführung von Informationssicherheits-Managementsystemen (ISMS) und umfasst u.a.: scoping, boundaries and ISMS policy, requirements analysis, risk assessment / risk treatment, design the ISMS, responsibilities, internal auditing, policy structure, measuring.

Kritische Geschäftsprozesse

ISO 27003 gleicht einer „Bauanleitung mit Strukturplan“, mit dem die ISMS-Implementierung paketweise abgearbeitet werden kann, meint Herfried Geyer. Die durchaus kontroversiellen Abhandlungen unterstützen bei der zentralen Frage: „Welche Normforderungen des Zertifizierungsstandards ISO 27001 sollen in welcher Tiefe ausgearbeitet werden und warum“. Gene¬rell liegt der Fokus darauf, Informationssicherheit direkt an Business Prozessen auszurichten. „Security soll kein Selbstzweck sein. Das kommt in ISO 27003 klar zum Ausdruck“, so der CIS-Auditor. Dies beginnt laut Kapitel 6 bei einer sauberen Definition des zu zertifizierenden Bereiches: Demnach sind kritische Geschäftsprozesse in das Scoping aufzunehmen, auch wenn sie Organisationsgrenzen überschreiten wie bei Budgeting und Accounting, Zulieferung oder Auslieferung.

Abbildung 1. *Dipl.-Ing. Herfried Geyer ist Auditor der weltweit tätigen Zertifizierungsorganisation CIS mit Sitz in Wien.*

Von Business Analyse bis Risiko

In Kapitel 7 „requirement analysis“ findet sich eine Anleitung für die Business Analyse als Basis für eine Risikoanalyse. Demnach sind Kerntätigkeiten des Unternehmens in Form von Geschäftsprozessen aufzulisten und zu klassifizieren. So wird sichergestellt, dass die Informationssicherheit an den Unternehmenszielen ausgerichtet wird. Erst dann erfolgt die in Kapitel 8 beschriebene Risikoanalyse, wo auf Risk Assessment und Risikominimierung eingegangen wird. Für Vertiefungen wird auf die RM-Subnorm ISO 27005 referenziert.

Strukturplan

Im Annex findet sich ein Implementierungsplan, der es ermöglicht, Projektschritte parallel oder seriell abzuarbeiten. CIS-Auditor Herfried Geyer: „Jeder Projektschritt ist in Teilschritte untergliedert, jeweils mit den Unterpunkten Input / Abwicklung / Output. So dient ISO 27003 als unterstützendes Instrument, um strukturiert und professionell Informationssicherheit auf internationalem Niveau zu implementieren.“

Webtipp: *www.cis-cert.com*

Kennzahlen: Wie effizient ist das Security-System?

Nach der Subnorm ISO 27004 lassen sich Kennzahlen für die Erfolgsmessung generieren. Aussagekräftige Zahlen stärken die Anerkennung von Informationssicherheit im Unternehmen.

Die Wirksamkeit von Maßnahmen im Rahmen eines Informationssicherheitsmanagementsystems (ISMS) wird erst durch Kennzahlen messbar und für das Management nachvollziehbar. Dies ist auch das Ziel der ISO/IEC 27004 für Measurement, eine Subnorm des Zertifizierungsstandards ISO 27001 für Informationssicherheit. „Das für Nicht-Experten nebulose Security-Thema wird mittels Kennzahlen greifbar und kann auf diese Weise einen breiteren Stellenwert im Unternehmen einnehmen“, argumentiert Normen-Experte Erich Scheiber, Geschäftsführer der akkreditierten Zertifizierungsorganisation CIS mit Hauptsitz in Wien. Durch Erfolgsmessung wird auch für andere Abteilungen sichtbar, zu welch hohem Grad die Informationssicherheit alle betrieblichen Bereiche durchdringt – vom Einkauf über das Marketing bis zur Personalverwaltung.

Methoden, Formeln, Analysen

ISO 27004 fungiert dabei als detaillierter Leitfaden für quantitative Erfolgskontrollen und Berichte, wodurch Prozessverbesserung nach „Plan-Do-Check-Act“ noch wirksamer und fokussierter wird. Der Standard bietet Messmethoden, mathematische Formeln, Definitionen für Basismaße und abgeleitete Maße, Analysetechniken sowie Entscheidungskriterien für aussagekräftige Security-Indikatoren.

…kombiniert mit Bauchgefühl

„Insgesamt ist die sehr methodische ISO 27004 nicht für die Eins-zu-Eins-Umsetzung konzipiert. Unternehmen profitieren, wenn sie Inhalte selektiv anwenden und mit ausgesuchten Kennzahlen beginnen“, führt CIS-Auditor Herfried Geyer aus. Teilweise lehnt sich der Inhalt am US-amerikanischen Gegenstück NIST SP 800-55 an, der allerdings mehr Raum für qualitative Bewertungen lässt. „NIST SP 800-55 ist gut mit ISO 27004 kombinierbar und gilt salopp formuliert als praktikable Funktionalisierung des Bauchgefühls“, meint Herfried Geyer.

Beispiele für Erhebungen

Wesentliche Security-Forderungen der Dachnorm ISO 27001 wie Monitoring von Sicherheitsmaßnahmen, Dokumentation von Messmethoden oder Evaluierung durchgeführter Schulungen werden mit ISO 27004 bestens erfüllt. Welche Arten von Kennzahlen sinnvoll sind, bleibt dabei dem Anwender überlassen. Beispiele sind je nach Policies und Situation:

- Kundenstammdaten-Integrität: Beschwerden in Prozent, Newsletter-Rückläufer in Prozent
- Schulungserfolg: Mitarbeiteranteil in Awareness--Programmen, Verständnis von vermittelten Inhalten in Prozent (Multiple Choise via Intranet)
- Third-Party-Agreements: Lieferanten-Anteil mit IS--relevantem Zuliefervertrag, Einhaltung/Nicht-Einhaltung, Problemquote
- Account Control: Fehlerquote bei User Accounts
- Sicherheitsvorfälle: Anzahl/Rückgang pro Jahr (Klassifizierung der Fälle nach ISO 27001)

Mehr Anerkennung

„Erfolgsmessung mittels Kennzahlen wird zu einer steigenden Anerkennung von Security-Anliegen und IS-Verantwortlichen im Unternehmen führen“, erwartet CIS-Geschäftsführer Erich Scheiber. Die „IT-lastige“ Informationssicherheit könne dadurch auch in den Augen andere Mitarbeiter zu einem ganzheitlichen Anliegen werden, das maßgeblich zum Unternehmenserfolg beitrage.

„Fehlertolerante Unternehmenskultur?“ Whistle Blowing aus Sicht der ISO 27001

Johannes Mariel

Personnel Security im Spannungsfeld von Schutz und Aufklärung: Ein Kommentar von Ing. Johannes Mariel, Bundesrechenzentrum

Im Spannungsfeld zwischen Schutz und Aufklärung findet sich die Informationssicherheit. In der Umgangssprache beschreibt „Whistle Blowing“ die nicht autorisierte Enthüllung vertraulicher Informationen – sei es aus Überzeugung oder für einen persönlichen Vorteil. Informationssicherheit hat das Ziel, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen „angemessen“ zu schützen. Inwieweit kann also die Umsetzung des internationalen Security-Standards ISO/IEC 27001 einem Phänomen wie dem ungewollten Veröffentlichen betrieblicher Informationen vorbeugen und gleichzeitig Transparenz im Unternehmen etwa im Rahmen eines Meldewesens ermöglichen?

Personnel Security nach ISO 27001

ISO 27001 sieht zum sicheren Umgang mit Informationen ein Maßnahmenbündel zur Verpflichtung der Beschäftigten auf die Sicherheitsregeln vor:

- Der Nutzer einer Information ist gemäß Anhang A „Klassifizierung von Informationen“ von der Vertraulichkeit von Informationen in Kenntnis zu setzen. Dafür sind Richtlinien für Klassifizierung und Kennzeichnung zu erstellen.
- Die Mitarbeiter sind gemäß Kapitel 8.1 „Personelle Sicherheit“ vor einer Anstellung auf ihre Vertrauenswürdigkeit zu überprüfen, in Abstimmung mit den Risiken eines Vertrauensbruchs.
- Während der Beschäftigung sind die Mitarbeiter laut Kapitel 8.2. regelmäßig über relevante Sicherheitsregeln zu informieren.

Technik & „Faktor Mensch“

Die konsequente Umsetzung von Controls des Leitfadens ISO 27002 schafft den formalen Handlungsrahmen für ein Awareness-Programm. Dabei sind die Vorbildwirkung der Führungskräfte, risikospezifische Praxis-Workshops und Schwerpunkt-Aktionen effektive Bausteine einer Sicherheitskultur. Weitere ISO-27002-Controls wie die Regelungen der Zugriffskontrolle nach dem Need-to-Know-Prinzip, zur Aufgabentrennung oder zur Data Leakage Prevention sind wichtige Schutzmaßnahmen.

Riskmanagement & Fehlertoleranz?

Die Wirksamkeit aller dieser Maßnahmen ist letztlich aber von der persönlichen Akzeptanz der Mitarbeiter abhängig. Die Übereinstimmung der moralischen Werte eines Unternehmens mit denen seiner Mitarbeiter ist ein bestimmender Faktor für die Schwelle, die Whistle Blower überschreiten. Hier entfaltet die ISO-27000-Familie ihre eigentliche Stärke als ein Regelwerk, das keine starren Vorgaben definiert, sondern kreative Denkprozesse anstößt, vor allem auch über das Instrument des Risikomanagements: Stellt eine Organisation sicher, dass das Fehlverhalten Einzelner bei Bekanntwerden geahndet wird, reduziert dies das Risiko von Whistle Blowing deutlich. Eine fehlertolerante Kultur mit einer klaren Unterscheidung zwischen absichtlichem Fehlverhalten und entschuldbaren Fehlern nach dem Grundsatz „Jeder Sicherheitsverstoß hat eine Ursache, aber nur wenige haben ein persönliches Verschulden“ schafft zufriedene und loyale Mitarbeiter.

JOHANNES MARIEL

Ing. Johannes MARIEL, CSO der Bundesrechenzentrum GmbH in Wien, zeichnet für das Informationssicherheitsmanagementsystem im BRZ verantwortlich.

„Wolkig bis trüb“: Datenschutz bei Cloud Computing

Karin Peyerl

Vom Newsletter-Tool bis zur ERP-Software verzeichnen Cloud Services zweistellige Wachstumsraten, bergen aber auch neue Risiken. Bei Datenpannen „in der Wolke“ ist der Nutzer für die Auswahl seines Providers haftbar. Haftungsminimierung wird erreicht, wenn ein Cloud-Provider nach ISO 27001 zertifiziert ist und der Standard vertraglich aufgenommen wird.

Aktuelle Studien zu Folge boomt Cloud Computing mit zweistelligen Wachstumsraten. Für das Jahr 2010 hat Gartner einen weltweiten Umsatz mit Cloud Services von 58,6 Mrd. US$ ermittelt, der bis 2014 auf 148,8 Mrd. US$ ansteigen soll. Noch sind sich Unternehmen aber kaum der neuen Risiken bewusst, denn bisher gibt es weder gesetzliche Regelungen noch Richtlinien für die „Datenverarbeitung in der Wolke“.

Laut Forrester Research steht Cloud Computing für „*verwaltete IT-Infrastruktur, die Anwendungen via Internet bereitstellt und nach Gebrauch abgerechnet werden kann*“. Dazu gehören „Software as a Service“-Dienste wie CRM-, ERP-, Kollaboration- oder Newsletter-Tools. Aber auch Rechen- und Speicherlösungen sowie Entwicklungsplattformen. Der finanzielle Vorteil aufgrund standardisierter, webbasierter Anwendungen birgt den Nachteil, dass die gemeinsame Nutzung der Ressourcen durch mehrere Vertragspartner nicht transparent ist. Das Risiko steigt noch, wenn unbekannte Sub-Provider Kapazitäten beistellen.

ISO 27001: Zertifizierung von Informationssicherheit

Der internationale Standard ISO/IEC 27001 ermöglicht ein strukturiertes Managementsystem für Informationssicherheit mit hochsicheren Daten und hochverfügbarer IT. Der Standard umfasst neben technischen Aspekten auch Organisation, Mitarbeiter-Awareness oder physische Sicherheit wie Gebäudeschutz. Die Umsetzung erfolgt mittels Risikoanalyse, Daten-Klassifizierung, Policies und Maßnahmenkontrolle nach dem Prozessmodell Plan-Do-Check-Act. Gemäß dem gesetzlichen Sorgfaltsgrundsatz reduziert eine ISO-27001-Zertifizierung das Haftungsrisiko. Eine der führenden Zertifizierungsorganisation in Zentral- und Osteuropa ist „CIS - Certification & Information Security Services“. www.cis-cert.com

Nutzer haftet für die Auswahl des Providers

Wer haftet bei „Datenpannen“ in der Wolke? Und inwieweit hilft eine Zertifizierung des Providers nach dem internationalen Security-Standard ISO 27001 die Haftung zu reduzieren? Die EU-Datenschutz-Richtlinie sieht zwar vor, dass Unternehmen Dienstleister wie Cloud-Provider in Anspruch nehmen können. Das aber nur, wenn diese „eine rechtmäßige und sichere Datenverarbeitung“ gewährleisten. Faktisch heißt das: Der Cloud-Nutzer haftet – je nach Umsetzung der EU-DSR in nationales Rechts – für die Auswahl des Providers. Das Unternehmen muss demnach aktiv einen „Security-Nachweis“ verlangen, wozu es zwei Möglichkeiten gibt: Durchführung von Dienstleister-Audits oder Einfordern eines Zertifikates, welches durch eine akkreditierte Prüforganisation ausgestellt wurde. Zu den führenden Zertifizierungsorganisationen für ISO 27001 in Zentral- und Osteuropa gehört die CIS.

Haftungsminimierung durch ISO 27001

Ist ein Provider nach ISO 27001 zertifiziert, bedeutet dies für den Cloud-Nutzer, dass sein Provider Datenschutzverpflichtungen mit „größtmöglicher Sorgfalt“ erfüllt, wodurch sich das Haftungsrisiko bei Datenpannen auf beiden Seiten minimiert. Denn der Security-Standard umfasst die Einhaltung anzuwendender Gesetze als Prüfkriterium, was aufgrund der „Third Party“-Anforderungen der Norm auch für involvierte Sub-Provider gilt. ISO-27001-zertifizierte Unternehmen verpflichten sich zur Einhaltung der Legal Compliance in all jenen Ländern, in denen Kundenbeziehungen bestehen.

Generelle Gefahren „in der Wolke“

Da es noch keine spezifischen Regelungen zu Cloud Computing gibt, ist es für Nutzer schwierig, alle Rechtsaspekte zu berücksichtigen. Aus Datenschutz-Sicht sind folgende Punkte relevant:

„Take it or leave it“-Verträge

Für standardisierte Services sind die AGB meist nachteilig für Nutzer, insbesondere in Bezug auf Haftungsfragen bei Datenverlust und -rückführung sowie Zugriffs- und Kontrollrechten. Ein Provider sollte daher ein Sicherheitskonzept vertraglich zusichern. Empfehlenswert ist der Abschluss von Service Level Agreements (SLA) oder die vertragliche Integration von ISO 27001 als Maßstab für die Leistungserbringung.

Mangelnder Schutz im Ausland

Räumlich knüpft die EU-Datenschutzrichtlinie primär an den Ort der Datenverarbeitung an, wonach Cloud-Provider mit Sitz im EU-/EWR-Raum die gesetzlichen Datensicherheitsmaßnahmen zu erfüllen haben. Bei Anbietern außerhalb des EU-/EWR-Raums besteht keine Verpflichtung zur Einhaltung des EU-Datenschutzrechts. Zudem können durch eine Datenüberlassung außerhalb des EU-/EWR-Raums behördliche Genehmigungspflichten entstehen, deren Nicht-Einhaltung mit Verwaltungsstrafen geahndet werden.

Unkenntnis über Datenstandort

Die Auslagerung von Daten an Provider entbindet Cloud-Nutzer nicht von ihrer „Verpflichtung zur Sicherstellung der Datensicherheit“. Maßnahmen wie Zugriffskontrollen oder das Recht auf Auskunft und Löschung von Daten können aber nicht gewährleistet werden, wenn der Ort der Speicherung aufgrund verteilter Ressourcen nicht bekannt ist. Ebenso problematisch ist, dass kaum einheitliche Log-Files generiert werden, wodurch die Protokollierung von Verwendungsvorgängen wie Abfrage, Änderung und Übermittlung von Daten erschwert wird. Bei einem ISO-27001-zertifizierten Provider kann sichergestellt werden, dass dieser normgemäß Protokollierungen und Archivierung von Log-Files durchführt und es auch von seinen Sub-Providern vertraglich einfordert.

Auswahl des Cloud-Anbieters

Datenpannen können Schadenersatzforderungen in Millionenhöhe verursachen, wie Fälle bei Banken und Versicherungen zeigen. Aus juristischer Sicht sind daher nur Cloud-Anbieter empfehlenswert, die sich vertraglich zur Datensicherheit verpflichten und eine externe Zertifizierung vorweisen, wodurch an deren Sub-Anbieter wichtige Datenschutzverpflichtungen übertragen werden.

KARIN PEYERL

ist Rechtsanwältin bei der CHSH in Wien, Österreich, tätig und hat ihre Schwerpunkte im Datenschutz-, IT- und Arbeitsrecht. www.chsh.com

Die neue Epoche der Datenverschlüsselung

Kilian Zantop

Netzwerkverbindungen werden fälschlicherweise als vertrauenswürdig erachtet.

IN DIESEM ARTIKEL ERFAHREN SIE...

- Konsistenter Einsatz von Verschlüsselung ist im Trend. Nachstehend erfahren Sie das Wichtigste über Verschlüsselungstechnologien, Vor- und Nachteile davon sowie was der Einsatz Unternehmen bedeutet. Zudem erhalten Sie wertvolle Informationen, Datenverschlüsselung auch einfach und kostengünstig umgesetzt werden kann.

WAS SIE VORHER WISSEN SOLLTEN...

- keine Vorkenntnisse notwendig

Die sichere Übermittlung von Nachrichten ist kein neues Thema, sondern geht weit ins Mittelalter zurück. Schon in der Antike gab es zusammengerollte Schriftstücke. Um die Intimität von Information zu erhöhen, bediente man sich in weiterer Folge des Briefumschlags. Zudem wurden früher wichtige Dokumente im Tresor aufbewahrt. Doch heute liegen diese sensiblen Informationen meistens ungesichert in Firmennetzwerken. Oftmals fehlt dabei das Bewusstsein, was mit solch leicht zugänglichen Daten passieren kann.

Letztendlich geht es immer um die Privatsphäre, sei es die persönliche oder die geschäftliche. Niemand ist daran interessiert, dass sensible Informationen (z.B. Finanzdaten, Kundendaten, Forschungs- und Entwicklungsdaten, eMails oder aber auch Bilder, Videos, Passwörter, (Liebes)briefe, Tagebücher uvm.) in die Händen von Fremden oder gar Kriminellen geraten. Netzwerke sind grundsätzlich als unsicher zu betrachten. Sie müssen deshalb präventiv vor unberechtigtem Zugriff geschützt werden.

Sicherheitsrisiken haben stark zugenommen. Reine Perimeter-basierende Sicherheitsansätze (nur an den Übergängen vom Netzwerk) bieten heute nicht mehr den benötigten Schutz vor Datenverlust oder -missbrauch. Obwohl Firewalls, Antivirenprogramme, Intrusion Detection Systeme, Authentifizierungslösungen etc. auch weiterhin grundlegende Technologien in einem Sicherheitskonzept bilden, müssen Daten künftig vor allem auch auf den Übertragungswegen geschützt werden. Unternehmen müssen sich verstärkt mit Themen wie dem unerwünschten Datenabfluss, Insiderattacken und Angriffen von aussen befassen.

In der Vergangenheit machten sich weder Privatleute noch Unternehmen grosse Gedanken um die Datensicherheit bei Netzwerkverbindungen, weil diese fälschlicher Weise als sicher galten. Dabei sind Mängel offensichtlich. Verbindungen über öffentlichen Grund oder auch in öffentlich zugänglichen Treppenhäusern können leicht angezapft werden: Anleitungen zum Anzapfen von Netzwerken stehen im Internet zum Download bereit und die dafür benötigten Utensilien lassen sich problemlos beschaffen. Nur die Datenverschlüsselung der Netzwerkkommunikation kann hierbei sensible Informationen vor neugierigen Blicken und Manipulationsversuchen effektiv schützen. Wird der Datenschutz an die Daten gekoppelt, ist auch der Datenfluss kontrollierbar.

Der Status Quo der Datenverschlüsselung

Konsistenter Einsatz von Verschlüsselungstechnologien ist im Trend

Eine der wichtigsten Technologien im Bereich Datenschutz ist die Verschlüsselung von vertraulichen Informationen. Dies zeigt auch die Jahresstudie 2009 von PGP zum Thema „Verschlüsselungstrends in deutschen Unternehmen“, denn die strategische Planung von Verschlüsselung gewinnt weiter an Bedeutung. 31 Prozent

der Befragten gaben an, dass sie den konsistenten Einsatz von Verschlüsselungstechnologien unternehmensweit geplant haben. Als Hauptgrund wird von 46 Prozent der Befragten die Einhaltung des Datenschutzes für geistiges Eigentum genannt.

Das Thema Datenschutz beschäftigt die ganze Welt. In Deutschland wurden neue Gesetze ins Leben gerufen, welche die Meldung bei Datenschutzverletzungen verlangen. In gewissen Staaten in den USA wird für Gesundheitsdaten bereits Verschlüsselung zum Datenschutz vorgeschrieben. Die Zahl der Datenschutzgesetze nimmt laufend zu, ältere Gesetze werden überarbeitet und mit strengeren Vorschriften belegt. Auch das Bundesdatenschutzgesetzt BDSG-Novelle II unterstreicht die Bedeutung von Verschlüsselung als Massnahme der Zugangs-, Zugriffs- und Weitergabekontrolle.

Was man über Verschlüsselung wissen muss

Zusammengefasst beinhaltet die Kryptographie symmetrische und asymmetrische Kryptosysteme, auch Verschlüsselungsmethoden genannt.

Asymmetrische Verschlüsselung (auch Public Key Verfahren genannt)

Bei asymmetrischen Systemen wird für jeden Teilnehmer ein Schlüsselpaar generiert. Der eine Schlüssel davon wird öffentlich publiziert und kann von jedem Anwender für die Verschlüsselung von Nachrichten für den gewünschten Empfänger benutzt werden. Der zweite Schlüssel hingegen bleibt geheim und ist nur für den Empfänger verfügbar, der damit die Daten wieder entschlüsseln kann. Daher kommt auch die Bezeichnung „asymmetrisch“, da zwei verschiedene Schlüssel für die Ver- und Entschlüsselung benutzt werden.

Dieses Verfahren wird vor allem für E-Mail Verkehr sowie in kryptografischen Protokollen wie SSH oder SSL/TLS eingesetzt. Das bekannteste dieser Verfahren ist RSA.

Vorteile der asymmetrischen Verschlüsselung:

- Relativ hohe Sicherheit
- Vereinfachte Schlüsselübertragung nur Public Key wird übertragen und nur der private Schlüssel muss geheim gehalten werden
- Zudem können digitale Signaturen für die Authentifikation implementiert werden
- Anzahl der Schlüssel wächst „nur“ linear mit der Teilnehmerzahl

Nachteile der asymmetrischen Verschlüsselung:

- Die asymmetrische Verschlüsselung ist viel langsamer als symmetrische, dadurch ergibt sich ein geringerer Datendurchsatz.
- Auf Grund des öffentlichen Schlüssels ist eine höhere Schlüssellänge gefordert, um die Sicherheit zu gewährleisten.
- Die Erzeugung des Schlüssels ist komplexer, da „schwache“ Schlüsselpaare vermieden werden müssen.
- Verifizierung des öffentlichen Schlüssels kann nicht gewährleistet werden, da diese auch von einem Mittelsmann vorgetäuscht werden könnte. Implementierung von Prüfsummen oder Zertifizierungsstellen ist notwendig, um diesen Punkt sicherzustellen.
- Wird eine Nachricht an mehrere Teilnehmer übermittelt, muss diese für jeden Empfänger separat verschlüsselt werden, da ein anderer Public Key für die Entschlüsselung zum Einsatz kommt.
- Die Sicherheit von asymmetrischen Verfahren beruht auf unbewiesenen, jedoch von der Fachwelt anerkannten Annahmen.

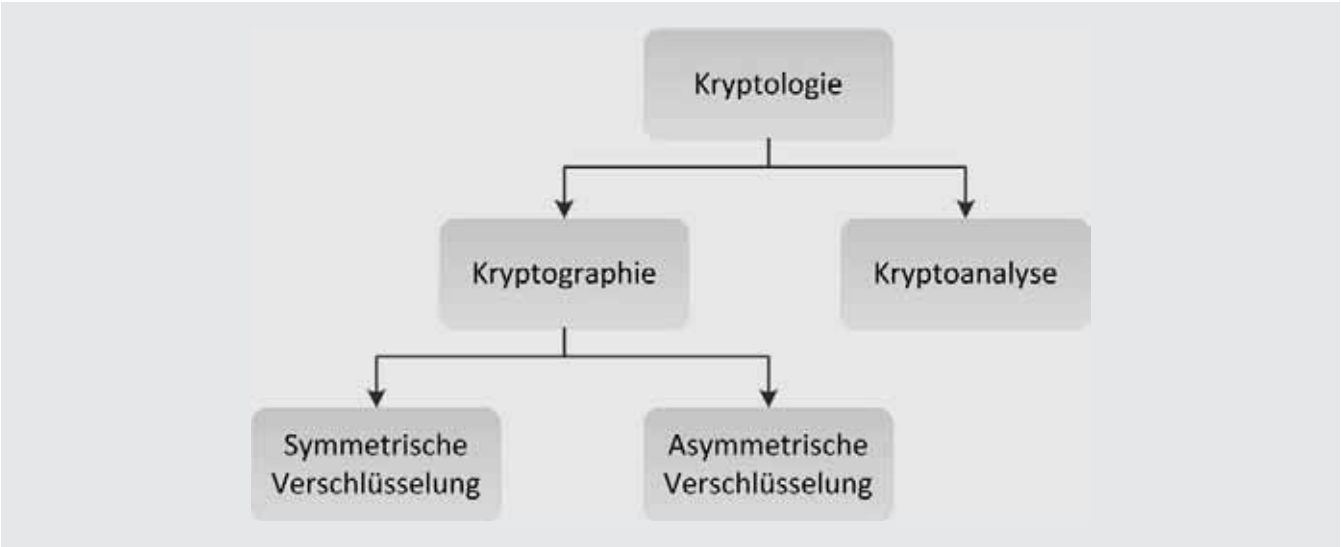


Abbildung1. *Kryptologie*

Symmetrische Verschlüsselung

Bei symmetrischen Systemen besitzen Sender und Empfänger den gleichen Schlüssel welcher zuvor sicher ausgetauscht werden muss. Zu den derzeitigen symmetrischen Verfahren gehören unter anderem auch die Cäsar-Chiffre, Twofish, 3DES, IDEA sowie Advanced Encryption Standard (AES).

Vorteile von symmetrischen Verfahren:

- Einfacheres Schlüsselmanagement, da nur ein Schlüssel für die Ver- und Entschlüsselung benötigt wird
- Höhere Geschwindigkeit für die Ver- und Entschlüsselung
- Gute symmetrische Verfahren sollten bis auf Brute-Force (Durchprobieren aller möglichen Schlüssel) allen anderen Attacken standhalten
- Höhere Sicherheit bei relativ kurzen Schlüsseln

Nachteile von symmetrischen Verfahren:

- Da nur ein Schlüssel für die Ver- und Entschlüsselung benutzt wird, darf dieser unter keinen Umständen in die falschen Hände gelangen
- Der Schlüssel muss über einen äusserst sicheren Weg übermittelt werden
- Die Anzahl der benötigten Schlüssel, bezogen auf die Anzahl Teilnehmer, wächst quadratisch
- Möglichkeit von Man-In-The-Middle-Attacken

Des Weiteren gibt es noch hybride Verfahren, welche die Vorteile von asymmetrischen und symmetrischen Verfahren kombinieren: Es wird eine asymmetrische Verschlüsselung benutzt um den Sitzungsschlüssel (Session Key) für ein symmetrisches Verfahren zu übertragen. Die Daten werden ebenfalls mit einem symmetrischen Verfahren verschlüsselt. Dieser Sitzungsschlüssel wird dann nur für eine Übertragung verwendet und anschliessend vernichtet. Das asymmetrische Schlüsselpaar kann hierbei auch über einen längeren Zeitraum im Einsatz bleiben.

Fazit: Bisher bekannte Verschlüsselungen haben sowohl Vor- wie auch Nachteile. Die Sicherheit bei der Übertragung des Schlüssels, sowie dessen Verwaltung, ist ein grosses Thema. Keine der bekannten Verschlüsselungen kann als „schnell“ bezeichnet werden. Auch der geringere Datendurchsatz führt zu unerwünschten Verzögerungen.

Die Sicherheit einer Verschlüsselung darf weder von der verfügbaren Rechenleistung noch von der Geheimhaltung des eingesetzten Algorithmus abhängig sein

Mankos bei Verschlüsselungen

Die Sicherheit eines Algorithmus wird von der Schwierigkeit abgeleitet, die notwendig ist, um diesen zu knacken sprich eine verschlüsselte Nachricht zu entschlüsseln. Diese Sicherheit sollte jedoch im Verhältnis zu dem Wert der verschlüsselten Daten stehen. Wenn der Aufwand, der für die Entschlüsselung eingesetzt werden muss, deutlich höher ist als der Wert der Daten, spricht man heute von einer relativen Sicherheit. Der eingesetzte Aufwand ist jedoch gleichzusetzen mit der Rechenleistung, welche eingesetzt werden muss, um mittels Ausprobieren von allen möglichen Kombinationen, den richtigen Schlüssel zu ermitteln. Die Problematik hierbei ist, dass sich das Angebot an Rechenleistung am Markt unglaublich schnell erhöht, Hardware günstiger wird und Systeme überholt sind. Das bedeutet, heute noch als sicher eingestufte Verschlüsselungen werden bald mit geringem Aufwand zu knacken sein.

Des Weiteren darf die Sicherheit einer Verschlüsselung nicht von der Geheimhaltung des eingesetzten Algorithmus abhängig sein. Wenn lediglich die Kenntnis vom Aufbau eines Algorithmus dazu führen würde, dass eine codierte Botschaft entschlüsselt werden kann, wäre die Gefahr viel zu gross. Die Sicherheit muss somit alleine durch die Geheimhaltung des Schlüssels gewährleistet werden, was zu Herausforderungen in Schlüsselmanagement führt.

Fazit: Es ist eine Verschlüsselungslösung nötig, bei welcher der Algorithmus, unabhängig der vorhandenen Rechenleistung, nicht zu knacken ist. Zudem sollte kein Schlüssel im eigentlichen Sinne mehr vorhanden sein, verwaltet und übertragen werden müssen, damit auch hier eine weitere Sicherheitslücke geschlossen werden kann.

Die Verwaltung des Schlüsselmaterials ist eines der Haupthindernisse für den Einsatz von Verschlüsselungs-lösungen

Die Kostenfrage

Die Kosten der Implementierung einer Verschlüsselungslösung, sind oftmals der grösste Knackpunkt für Kunden. Das Resultat ist, dass Daten, welche theoretisch verschlüsselt werden müssten, unverschlüsselt bleiben. In der Jahresstudie 2009 von PGP gaben 26 Prozent an, dass die Kosten der Verschlüsselungslösung das Haupthindernis für eine Einführung sind. 25 Prozent geben als Grund hierbei die Verwaltungskosten an. Als weitere Gründe werden auch Leistungseinbussen sowie die komplexe Verwaltung des Schlüsselmaterials angeführt. 34 Prozent der Befragten gaben an, über ein Jahr nur für die Planung der Schlüsselverwaltung benötigt zu haben.

Schlüsselmanagement

Für die Verwendung von Verschlüsselungslösungen wird normalerweise ein Schlüsselmanagement benötigt. Dieses Schlüsselmanagement, oder auch Schlüsselverwaltung genannt, ist für die vertrauliche Erstellung,

Verteilung sowie Installation von geeigneten Schlüsseln zuständig und verwaltet sämtliche Schlüssel über die gesamte Gültigkeitsdauer hinweg.

Auf der anderen Seite werden Investitionen in das Schlüsselmanagement als Massnahme zur Senkung der Betriebskosten gesehen. Man rechnet mit rund 32 Prozent des vorgesehenen Budgets, welche in das Schlüsselmanagement investiert werden müssen, was schlussendlich jedoch zu einer Gesamtbetriebskostensenkung für den unternehmensweiten Datenschutz führen wird.

Die Schlüsselverwaltung ist das A & O einer herkömmlichen Verschlüsselungslösung. Werden die Schlüssel beispielsweise nicht sicher genug verwaltet und ein Unbefugter kann sich Zugang dazu verschaffen, ist die Verschlüsselungslösung wertlos. Die entsprechenden Sicherheitsvorkehrungen für die Absicherung der Schlüsselverwaltung stellt ein scheinbar unlösbares Problem dar. Die Lösung wäre eine Verschlüsselung, welche keine Verwaltung und keine Übertragung im herkömmlichen Sinne mehr benötigt.

Verschlüsselungen müssen performanter werden.
Angst vor Performanceverlust

Immer wieder hört man von Performance-Einbrüchen, sobald eine Verschlüsselungslösung im Einsatz ist. Hierzu ein kleines Beispiel: Eine auf Layer 3 mit IPsec verschlüsselte Kommunikation wächst um rund 40 Prozent, bei Echtzeit-Anwendungen kann sogar ein Overhead von über 80 Prozent entstehen. Das Padding, also das Aushandeln des Schlüssels und der Aufbau des Tunnels, generiert bei herkömmlichen Lösungen einen kryptographischen Overhead. Dies führt unweigerlich dazu, dass die Netzwerkkommunikation ins Stocken gerät und weitere Kosten für zusätzlichen Bandbreitenbedarf anstehen. Im Falle von Echtzeit-Anwendungen führt dies allerdings auch nicht zu einer besseren Lösung.

Es sind einfache Lösungen gefragt – Komplexität muss der Vergangenheit angehören.
Einfache Lösungen sind die Zukunft

Verschlüsselungslösungen gelten grundsätzlich als sehr aufwendig. Komplexe Lösungen, sowie viele verfügbare Funktionen und Features, gehen mit hohen Kosten bei der Implementierung sowie auch bei den laufenden Betriebs- und Unterhaltskosten einher. Gemäss einer Studie der Firma d.velop AG haben sich 34 Prozent der Befragten dahingehend geäussert, dass sich Hersteller bei der Produktstrategie auf einfachere Implementierung, Bedienung und den Betrieb konzentrieren sollten. Mehr als drei Viertel der Befragten sind zudem der Meinung, dass der Implementierungsaufwand bei aktuellen IT-Lösungen viel zu hoch ist und fast gleich viele Teilnehmer geben dem Wartungsaufwand schlechte Noten.

Hersteller überfrachten ihre Produkte oftmals mit „Features & Functions“, welche jedoch meist nur zu einem kleinen Bruchteil genutzt werden können. Viele Funktionen bedeuten natürlich auch viele Codezeile. Je mehr Codezeilen vorhanden sind, desto mehr unbekannte Schwachstellen tun sich auf. Zudem können auch zusätzliche Fehler und damit wiederum mögliche Sicherheitslücken bei der Konfiguration entstehen.

Einfache Lösungen liegen daher wieder voll im Trend. Die Einfachheit bedeutet gleichzeitig einen geringeren Aufwand und damit auch geringere Kosten, was die Aufgabe von IT Verantwortlichen massiv vereinfacht.

Zusammenfassung

- Für die optimale Sicherheit muss der Datenschutz an die Daten geheftet werden.
- Strengere Datenschutzrichtlinien fördern den Einsatz von Verschlüsselungslösungen.
- Herausforderungen, welche jedoch zu bewältigen sind
- Aktuelle Verschlüsselungslösungen haben ihre Vor- und Nachteile, diese gilt es zu bewältigen.
- Neue Algorithmen, welche nicht mehr zu knacken sind, werden benötigt, egal wie viel eingesetzte Rechenleistung verfügbar ist.
- Das Schlüsselmanagement ist oftmals ein Hindernis für den Einsatz von Verschlüsselung: Neue Ansätze werden gebraucht.
- Verschlüsselungslösungen, welche die Performance beeinträchtigen, werden von Endbenutzern nicht geschätzt. Verschlüsselungen müssen generell leistungsfähiger werden, ohne dabei mehr Ressourcen zu benötigen.
- Der Markt braucht einfache Lösungen, welche in der Implementierung, der Administration sowie in den laufenden Betriebskosten möglichst wenige zu Buche schlagen.

Datenverschlüsselung gleichzusetzen mit Komplexität wäre ein Vorurteil
Datenverschlüsselung muss nicht komplex sein - Certus Lateo™ tritt den Beweis an

Datenverschlüsselung ist somit der einzige Weg, um sensible Informationen zu schützen. Denn verschlüsselte Daten sind auch in den Händen von Mitbewerbern oder anderen Unberechtigten schlichtweg wertlos. Wie erwähnt, bestehen aber die Vorurteile, dass Datenverschlüsselung komplexen Softwarelösungen, aufwendige Implementierungen und enormen Betriebsaufwand mit sich bringen. Auch besteht oftmals die Angst, die verschlüsselten Informationen nicht mehr entschlüsseln zu können.

Das Hause Barclay Technologies (Schweiz) AG hat sich dieser Problemstellungen angenommen und eine komplett neue Verschlüsselungstechnologie entwickelt. Dank des revolutionären Ansatzes wurde Datenverschlüsselung einfach, schnell und noch sicherer gemacht.

Barclay Technologies (Schweiz) AG ist ein aufstrebender Schweizer Hersteller der IT-Sicherheitsbranche und Entwickler einer komplett neuen und innovativen Verschlüsselungstechnologie. Mit dem Produkt Certus Lateo™ steht dem Markt ein völlig neuer Sicherheitsstandard im Bereich der Echtzeit-Datenverschlüsselung sowie der sicheren Netzwerkkommunikation zur Verfügung.

Die Technologie wurde zu 100% in der Schweiz entwickelt und in die Lösung integriert. Es besteht keine Pflicht zur Hinterlegung von Schlüsseln oder Algorithmen bei staatlichen Stellen und es unterliegen auch keine Exportrestriktionen.

Was ist Certus Lateo™?

Certus Lateo™ ist die smarte Lösung für den sicheren Schutz sensibler Daten

Certus Lateo™ ist ein einfach zu verwaltender Grundschutz. Sämtliche ein- und ausgehenden Daten werden auf den dafür vorgesehenen Rechnern innerhalb eines Netzwerkes verschlüsselt. Sobald Daten einen Rechner verlassen, um auf ein externes Speichermedium geschrieben zu werden, tritt die Verschlüsselung in Kraft und die Informationen sind für unautorisierte Dritte nicht verwertbar. Werden Daten auf einem Server abgerufen, wird der Datentransfer (Layer 3) ebenfalls verschlüsselt. Sensible Inhalte werden somit auch auf diesem Wege geschützt und nur für berechtigte Rechner nutzbar gemacht. Dank der innovativen Verschlüsselungstechnologie werden Daten „on the fly“ verschlüsselt. Für den Benutzer sowie auch im ganzen Netzwerk sind keinerlei Verzögerungen spürbar.

Es handelt sich um eine reine Software-Lösung. Diese wird in Form eines zusätzlichen Treibers auf unterster Systemebene installiert. Die Software ist nicht nur für die Ver- und Entschlüsselung jedes einzelnen Datenpaketes zuständig, sondern dient gleichzeitig als Authentifizierung. Damit erhalten nur noch definierte Teilnehmer Zugang zum Datentransfer und damit auf sensible Daten.

Certus Lateo™ wurde speziell für all diejenigen Unternehmen konzipiert, die eine Datensicherheitslösung einführen möchten, nicht aber über die notwendigen finanziellen sowie personellen Ressourcen verfügen, die bei der Implementierung einer herkömmlichen Data Loss Prevention Lösung erforderlich sind. Bei der Entwicklung wurde der Fokus auf die Einfachheit (Useability und Manageability) gelegt. Das Ziel war, Unternehmen einen raschen und kostengünstigen Schutz anbieten zu können. Features & Functions wurden hierbei auf ein nötiges Minimum beschränkt, damit auch die laufenden Administrations- und Betriebskosten so gering wie möglich ausfallen.

Die Vorteile von Certus Lateo™:

- Aufwände für die Datenklassifizierung entfallen
- Keine zusätzliche Passwort-Verwaltung
- Schlüsselverwaltung wird nicht benötigt
- Keine Interaktionen seitens des Benutzers
- Schulungsaufwand für Benutzer entfällt
- Sehr einfache, zentrale Policy-Verwaltung
- Keine Anpassungen der vorhandenen Netzwerkinfrastruktur notwendig
- Keine zusätzlichen Kosten für Hardware oder Backup-Infrastruktur

Sowohl die ungewollte oder mutwillige Verbreitung von sensiblen Daten über externe Massenspeicher, als auch das Abhören von übertragenen Daten im Netzwerk wird mit Certus Lateo™ zuverlässig und kostengünstig verhindert. Zudem wird durch die Verschlüsselung des Datentransfers ein „Trusted Environment“ gebildet, zu dem der Zugang nur durch die zusätzliche Authentifizierung mit dem Certus Lateo™ Treiber möglich wird. Damit steht ein erweiterter Schutz in folgenden Bereichen zur Verfügung:

- Zugangs-Authentifizierung der Rechner über Wireless
- Ungesicherte Kabelstränge über öffentliches Gelände sind abgesichert
- Gepatchte Netzwerkanschlüsse bedeuten keine Gefahr
- Zugang generell nur von authentifizierten Geräten – Rogue Access Points sind keine Gefahr mehr

Certus Lateo™ ist die smarte Datensicherheitslösung für einen effektiven Grundschutz, die in jedes Budget passt.

Funktionsumfang

Certus Lateo™ bietet Verschlüsselungs- und Sperrfunktionen für:

- Netzwerkverbindungen (LAN/MAN/WAN)
- WLAN
- Peer to Peer
- USB Sticks (Typen-unabhängig)
- Speicherkarten
- Speicher in mobilen Geräten
- Externe Festplatten
- CD/DVD/Blu-ray Laufwerke (Sperren der Schreibfunktion)

Eine neue Generation der Verschlüsselungstechnologie

Die innovative Technologie widerspricht allen gängigen Theorien von bekannten Verschlüsselungen und beschreitet neue Wege: Das Prinzip des One-Time-Pads in Kombination mit einem Schlüsselsystem, bei welchem der Schlüssel nicht mehr im herkömmlichen Sinne übertragen werden muss.

Key Facts der Verschlüsselungstechnologie

- Datenverschlüsselung
- bei welcher die Nachteile von aktuellen Verschlüsselungslösungen gelöst wurden
- Sichere Verschlüsselungs-technologie dank One-Time-Pad
- Ohne zusätzliches Schlüsselmanagement
- Real-Time-Verschlüsselung ohne spürbare Performance-Einbussen
- Sehr einfache Implementierung sowie Administrierung und damit geringe Gesamtprojektkosten
  - **Echtzeit-Verschlüsselung auf Paket- resp. Blockebene**
    Keine Verschlüsselung ganzer Dateien oder Datenträger, sondern Verschlüsselung jedes einzelnen Datenpakets/–blocks beim Verlassen des Systems.
  - **Dynamische Schlüsseltiefe pro Daten-Paket respektive Daten-Block bis zu 15‘048 Bit**
    Jedes Datenpaket wird mit einem individuellen Schlüssel in der gleichen Grösse wie das Paket selber verschlüsselt.
  - **Variable, dynamische Algorithmen**
    Für jedes Datenpaket wird mittels variablen, dynamischen Algorithmen ein völlig neuer Schlüssel in gleicher Grösse wie das Datenpaket selbst, generiert und angewandt.

Abbildung2. *Tresor mit Serverraum*

- **Kein Schlüsselaustausch im herkömmlichen Sinne**
  Sender und Empfänger sind im Besitz der Informationen, welche für die Ver- und Entschlüsselung benötigt werden, ohne dass diese im herkömmlichen Sinne übertragen werden müssen.
- **Kein Schlüsselaustausch im herkömmlichen Sinne und kein Key Management**
  Damit ist keine weitere Schwachstelle, vielmehr kein weiteres Angriffsziel vorhanden, was eine zusätzliche Absicherung erfordern würde.
- **Kein kryptographischer Overhead und keine Performance-Einbussen**
  Durch die einzigartige Verschlüsselungstechnologie werden keine spürbaren Performance-Einbussen generiert. Es erfolgt auch kein Handshake. Einerseits werden für den Verschlüsselungsvorgang die Ressourcen der Netzwerkkarte genutzt, andererseits werden keine ganzen Dateien auf den Systemen, sondern nur die Pakete beim Verlassen des Systems verschlüsselt.
- **Keine Wartungsfenster für Anpassungen notwendig**
  Da Paket-basierend verschlüsselt wird, kann die Verschlüsselung während des laufenden Betriebes ein oder ausgeschalten werden. Ein Paket kann verschlüsselt, das nächste unverschlüsselt ankommen, ohne dass dies Auswirkungen auf die Gesamtkommunikation hat.

Die neuartige Verschlüsselungstechnologie kombiniert damit die Sicherheit des One-Time-Pads mit der zusätzlichen Sicherheit aus der „Nichtübertragung" des Schlüssels.

Eine simple Datensicherheitslösung

Datenschutzlösungen gibt es bereits diverse und Data Loss Prevention oder Data Leakage Prevention (DLP) wird von zahlreichen Herstellern angeboten. Damit solche Lösungen jedoch implementiert werden können, muss man sich zuerst im Klaren sein, über welche Wege Datenverluste entstehen können. Man muss sich auf eine mehrstufige Vorgehensweise einstellen, sprich auf eine umfassende Analyse und einen projektbasierenden Ansatz. Soll ein umfassender Schutz von sensiblen Daten gewährleistet sein, reicht eine DLP Lösung alleine, von welchem Hersteller auch immer, bei weitem nicht aus.

Certus Lateo™ hat einen komplett anderen Ansatz und basiert weder auf einer Datenklassifizierung noch auf einer anderen Methode, um sensible Daten zu identifizieren. Es werden damit auch keine umfassenden Daten-Analysen benötigt, welche eine anschliessende Überwachung überhaupt erst möglich machen.

Certus Lateo™ ist die simple Datensicherheitslösung für alle Unternehmen, die rasch einen kostengünstigen und effizienten Schutz für ihre sensiblen Daten implementieren wollen.

Digitale Geschäftsabläufe versus Datenschutz

Das 21. Jahrhundert hat viel Bewegung in die Informationstechnologie gebracht. Immer mehr Geschäftsabläufe werden auf digitalem Wege abgebildet, Geschäftsprozesse werden in Software-Lösungen umgesetzt und das Kapital eines Unternehmens – sprich die Daten – liegt nicht mehr im Tresor wie früher, sondern oftmals schutzlos im Unternehmensnetzwerk. Datenmissbrauch und Datendiebstahl sind die neuen Schlagwörter der Medien und ein Ende der neuen digitalen Bedrohungen ist noch nicht in Sicht. Doch lässt sich wirksamer Datenschutz und Datensicherheit überhaupt mit digitalen Geschäftsabläufen vereinbaren?

Flexibilität versus Sicherheit

Mitarbeiter verlangen heutzutage grösstmögliche Flexibilität in ihren Arbeitsprozessen. Einschränkungen in den Abläufen, zusätzliche Auflagen für den Umgang mit gewissen Hilfsmitteln im täglichen Geschäftsalltag oder gar Restriktionen wirken oft hinderlich. Den wenigsten Unternehmen ist jedoch bewusst, dass zu viel Flexibilität in der Handhabung von Daten für die Sicherheit eine enorme Bedrohung darstellt. Sicherheit ist meist das pure Gegenteil von Flexibilität, denn sie besteht aus straffen Regeln. Jede Ausnahme dieser Regeln stellt ein hohes Gefahrenpotenzial dar und kann dazu führen, dass Geschäftsgeheimnisse auf einer Internet-Plattform oder direkt beim Konkurrenten landen. Handelt es sich hierbei um eine geheime Rezeptur für ein Medikament, von welchem sich ein Unternehmen den Marktdurchbruch erhofft oder eine Preiskalkulation, mit welcher der überlebensnotwendige Grossauftrag gewonnen werden soll, kann dies erhebliche Folgen haben. Zuviel unbedachte Flexibilität bei Arbeitsabläufen kann somit fatale Folgen haben.

Wie können sich Unternehmen absichern?

Es gibt verschiedene Ansätze um sich vor Datenverlust/-diebstahl zu schützen. Einer der bekanntesten ist Data Loss Prevention oder auch Data Leakage Prevention. Mit diesen Lösungen lassen sich die Ausnahmen, welche die gewünschte Flexibilität der Mitarbeiter weitgehend berücksichtigen, am ehesten abbilden. Schon alleine die Umsetzung eines hierfür notwendigen Gesamtkonzeptes ist jedoch mit derart hohen Aufwänden verbunden, dass entsprechende Projekte oftmals gar nicht ernsthaft erwogen werden können.

Folgende Schritte sind für die Umsetzung notwendig: Man muss sich zuerst bewusst werden, welche Daten wo vorhanden sind und diese in spezifische Gefahrenklassen einstufen. Damit dies umgesetzt werden kann, muss jeweils der ursprüngliche Datenbesitzer/-erstel-

ler ermittelt werden, welcher bestimmen muss, wie kritisch die Informationen sind. Erst dann kann die eigentliche Einstufung der Information in die entsprechende Gefahrenklasse vorgenommen werden. Diese Aufgabe bedeutet für viele Unternehmen bereits einen Aufwand, welcher kaum zu bewältigen ist. Man denke nur an die vielen Terabyte Daten, welche sich über Jahre an den verschiedensten Orten in den Datenbanken des Unternehmens angesammelt haben.

Der nächste Schritt ist die Ermittlung des Datenflusses, sprich welcher Mitarbeiter welche Daten auf welchen Wegen (Abspeichern auf mobilen Datenträgern, Versenden per Email etc.) in seinem Arbeitsalltag benutzt. Wer ist nach wie vor befugt auch kritische Informationen unverschlüsselt auf einem USB Stick abzuspeichern, da er Informationen beispielsweise dem Treuhänder übergeben muss? Wer darf Offerte nach wie vor unverschlüsselt per Email versenden?

Erst wenn diese beiden vorbereitenden Prozesse durchgeführt bzw. definiert sind, kann anschliessend eine Matrix mit den benötigten Sicherheitsrichtlinien definiert werden. In dieser Matrix wird abgebildet, wer künftig mit welchen Daten noch welche Aktionen in welcher Form durchführen darf. Beispielsweise darf Benutzer A Informationen der Klasse B nach wie vor unverschlüsselt auf einen USB Stick speichern, Informationen der Klasse D jedoch nur noch verschlüsselt. Ist diese Matrix vorhanden, kann diese in einer Data Loss Prevention Lösung abgebildet und im Unternehmen implementiert werden. Damit lassen sich die vorgegebenen Sicherheitsrichtlinien elektronisch durchsetzen und können auch überwacht werden.

Data Loss Prevention zu implementieren ist nur der erste Schritt

Mit der Implementierung einer solchen Lösung ist die Aufgabenstellung jedoch noch lange nicht abschliessend erfüllt. Jede neu erstellte Datei muss klassifiziert werden, damit die richtigen Sicherheitsrichtlinien bei der Verwendung greifen können. Jeder Mitarbeiter muss entsprechend geschult werden, damit er das System versteht und auch gemäss den Richtlinien anwenden kann. Es ist ein konstanter, fortlaufender Prozess der Klassifizierung von Daten- und Benutzern. Man denke nur an eine Pressemitteilung, welche vor dem Zeitpunkt der Veröffentlichung geheime Informationen beinhaltet und nach der Veröffentlichung jedem zugänglich sein muss. Damit ist der Aufwand auch nach der Implementierung enorm hoch und die Lösung kann nur wirksam sein, wenn alle Prozesse kontinuierlich überprüft, angepasst und auch umgesetzt werden.

Problematik IT Budget

Der Wert von IT-Sicherheit lässt sich nicht leicht finanziell messen und der Aufwand, der betrieben werden muss, steht oftmals in keinem Verhältnis zu den eigentlich so einfach klingenden Anforderungen. Das Management ist sich der Komplexität seiner Forderung an die IT Abteilungen selten bewusst. Aus diesem Grund ist auch das notwendige Budget für die IT-Sicherheit nicht im erforderlichen Masse vorhanden. Sicherheitsverantwortliche stehen damit in einem Spannungsfeld zwischen Anwenderwünschen, also der geforderten Flexibilität, und kostenorientierten Lösungen zum Schutz von versehentlichen oder böswilligem Datenabfluss. Die Herausforderung für den Sicherheitsverantwortlichen ist gross.

Digitale Geschäftsabläufe versus Datenschutz

Es ist offensichtlich, dass digitale Geschäftsabläufe kaum mit Datenschutz unter einen Hut gebracht werden können. Die Lösungen, welche die geforderte Flexibilität gewährleisten, benötigen sowohl enorme personelle als auch finanzielle Ressourcen, welche einem IT Verantwortlichen nur in wenigen Fällen zur Verfügung stehen. Damit muss entweder auf die Flexibilität verzichtet und auf einfache, kostengünstige Lösungen zurückgegriffen werden. Verzichtet man grundsätzlich auf Datenschutzlösungen besteht das Risiko, dass sensible Informationen in falsche Hände geraten, etwa in die der Konkurrenz oder in die der Öffentlichkeit (wie zum Beispiel über WikiLeaks).

Grundsätzlich sollten sich Unternehmen die Frage stellen, ob die Flexibilität, allen Mitarbeitern ungefiltert Datenzugänge zu gewähren in diesem Ausmass notwendig ist. Es sollte Bewusstsein darüber herrschen, dass es theoretisch Mitarbeiten möglich ist, mit einen USB Stick kritische Daten aus der sicheren Umgebung zu entfernen. Einfache Lösungen, die weder in der Implementierung noch in der Administration zu komplex sind, können die besten Ansätze liefern. Selbstverständlich müsste die gewünschte Flexibilität in den digitalen Geschäftsabläufen zu Gunsten des Datenschutzes zurückstecken. Im Sinne der Datensicherheit, lässt sich eine Vereinbarung beider Punkte nicht umsetzen.

KILIAN ZANTOP

Der Autor ist Chief Technical Officer bei der Barclay Technologies (Schweiz) AG. Sein Verantwortungsgebiet umfasst unter anderem die Weiterentwicklung des Produktes Certus Lateo™, welches auf einer einmaligen Verschlüsselungstechnologie aus dem Schweizer Hause Barclay Technologies basiert. Er ist seit über 20 Jahren in verschiedenen verantwortungsvollen Positionen in der IT unterwegs, wobei er sich in den letzten zwölf Jahren vor allem auf das Schwerpunktthema Security konzentriert hat.

Kontakt mit dem Autor: kilian.zantop@barclaytechnologies.ch

Recommended Sites

Datenschutz ist EU-weit gesetzliche Anforderung. Wir sorgen für die Erfüllung rechtlicher Vorschriften und kümmern uns um ein angemessenes Datenschutzniveau in Ihrem Unternehmen, auch international.

www.blossey-partner.de

Die Netzwerktechnik steht auf www.easy-network.de im Mittelpunkt. Artikel, Tutorials und ein Forum bieten genügen Stoff für kommende Administratoren und Netzwerkprofis.

www.easy-network.de

Die Seed Forensics GmbH bietet für Strafverfolgungsbehörden professionelle Unterstützung in den Bereichen der Datensicherstellung und Datenträgerauswertung. Selbstverständlich entsprechen unsere Mitarbeiter, unser technisches Equipment und auch unsere Räumlichkeiten den notwendigen Anforderungen.

www.seed-forensics.de

Securitymanager.de ist eine Produktion des Online-Verlag FEiG & PARTNER. Seit dem Start hat sich Securitymanager.de zu einem führenden Online-Informationsportal in Deutschland entwickelt und versteht sich als unabhängiger Informationsdienstleister der IT- und Information-Security-Branche.

www.securitymanager.de

Happy-Security ist ein neues Portal mit Security-Challanges, IT-Quiz, Web-Bibliothek, Multimedia-Center & vielen weiteren Features.

www.happy-security.de

Hier findest Du alles, was das Herz eines Computerfreaks höher schlagen lässt: Geek Wear mit intelligenten Sprüchen, eine riesige Auswahl Gadgets und natürlich auch viele Hacker Tools.

www.getDigital.de

Pericom base camp IT-Security: Unser Ziel ist es, unsere Kunden vor möglichen Gefahren für Ihre IT-Infrastruktur bestmöglich zu schützen. Neben der Analyse von Risikopotentialen durch Security Audits bieten wir, durch die Implementierung von Security-Lösungen, Schutz vor konkreten Gefahren.

www.pericom.at

CloudSafe stellt seinen Nutzern eine Plattform zur kryptographisch sicheren Ablage und Verwaltung von sensiblen Daten zur Verfügung: Nutzer können auf CloudSafe beliebig viele Dokumente in virtuellen Safes ablegen. Es können weiteren Personen individuelle Zugriffsrechte auf die Safes eingeräumt und somit ein sicherer Datenaustausch ermöglicht werden.

www.cloudsafe.com

AV-Comparatives geht hervor aus dem Innsbrucker Kompetenzzentrum und gilt als eines der bekanntesten unabhängigen Testhäuser für Antiviren-Software.

www.av-comparatives.org

Wollen Sie Ihre Seite empfehlen, kontaktieren Sie bitte: *de@hakin9.org*

Recommended Companies

Mabunta

Die mabunta GmbH agiert als hochspezialisierter und kompetenter Partner rund um IT-Security- und Netzwerk-Lösungen. Wir unterstützen bei IT-Sicherheitsfragen in allen Unternehmensbereichen, verbinden Wachstum mit sicherer Kommunikation.
Alles in allem- mabunta „one-face-to-the-customer“, Ihr Spezialist in Fragen der IT-Sicherheit.

www.mabunta.de

secXtreme GmbH

schützt Ihre Web-Anwendungen bis auf Applikationsebene. Dazu gehört sowohl die Prüfung von Applikationen (Pentests und Code-Reviews) als auch Beratungsleistungen für Sicherheit im Entwicklungsprozess und Schutzlösungen (Web Application Firewalls) bei Großunternehmen und dem gehobenen Mittelstand.

www.sec-Xtreme.com

SEC Consult

SEC Consult ist der führende Berater für Information Security Consulting in Zentraleuropa. Die vollständige Unabhängigkeit von SW- und HW-Herstellern macht uns zum echten Advisor unserer Kunden. Unsere Dienstleistungen umfassen externe/interne Sicherheitsaudits, (Web-) Applikationssicherheit (ONR 17-700), Sicherheitsmanagement-Prozesse (ISO 27001) etc.

www.sec-consult.com

B1 Systems

Die B1 Systems ist international tätig in den Bereichen Linux/Open Source Consulting, Training und Support. B1 Systems spezialisiert sich in den Bereichen Virtualisierung und Cluster.

info@b1-systems.de
www.b1-systems.de

Tele-Consulting GmbH

Vom BSI akkreditiertes Prüflabor für IT-Sicherheit, hakin9 und c't Autoren, jahrelange Erfahrung bei der Durchführung von Penetrationstests und Security-Audits, eigener Security Scanner „tajanas”, Sicherheitskonzepte, Risikoanalysen, IT-Grundschutz-Beratung, 3 lizenzierte ISO 27001-Auditoren, VoIP-Planung und -Security

www.tele-consulting.com

Blossey & Partner Consulting Datenschutzbüro

Datenschutz ist EU-weit gesetzliche Anforderung. Wir sorgen für die Erfüllung rechtlicher Vorschriften und kümmern uns um ein angemessenes Datenschutzniveau in Ihrem Unternehmen, auch international. Wir erledigen alle erforderlichen Aufgaben, die Fäden behalten Sie in der Hand. Nutzen Sie unser Erstberatungsgespräch.

www.blossey-partner.de

Recommended Companies

NESEC

NESEC ist Ihr Spezialist für Penetrationstests, Sicherheitsanalysen und IT-Security Counsulting. Das NESEC Pentest-Team unterstützt Sie bei Sicherheitsprüfungen Ihrer Netzwerke und Webapplikationen sowie bei Source Code Audits. Bei Bedarf optimieren wir Ihre Policy, sensibilisieren Ihre Mitarbeiter und zertifizieren Ihr Unternehmen nach ISO 27001.

www.nesec.de

m-privacy GmbH

IT-Sicherheitslösungen – funktional und einfach zu bedienen!
So präsentieren sich die von m-privacy entwickelten TightGate™-Server, z.B. TightGate™-Pro mit Datenschutz-Gütesiegel. Es bietet als erstes System weltweit einen kompletten Schutz vor Online-Spionage, Online-Razzien und gezielten Angriffen!

www.m-privacy.de

Seed Forensics GmbH

Die Seed Forensics GmbH bietet für Strafverfolgungsbehörden professionelle Unterstützung in den Bereichen der Datensicherstellung und Datenträgerauswertung. Selbstverständlich entsprechen unsere Mitarbeiter, unser technisches Equip-0ment und auch unsere Räumlichkeiten den notwendigen Anforderungen.

www.seed-forensics.de

OPTIMAbit GmbH

Wir sind Spezialisten für Entwicklung und Security. Wir sichern Java, .NET und Mobile Applikationen gegen Angriffe externer und interner Art. Unsere Dienste umfassen Audits, Code Reviews, Penetrationstest, sowie die Erstellung von Policies. Zusätzlich bieten wir Seminare zu sicherheitsrelevanten Themen.

www.optimabit.com

Protea Networks

Protea ist spezialisiert auf IT-Security-Lösungen: Verschlüsselung, Firewall/VPN, Authentifizierung, Content-Filtering, etc. Wir bieten umfassende Beratung, Vertrieb von Security-Hard- und Software, Installation und umfangreiche Dienstleistungen (z. B. Konzeption, Trainings). Protea setzt auf Lösungen der Markt- und Technologieführer und hält dafür direkten inhouse-Support bereit.

www.proteanetworks.de

secadm

secadm ist durchtrainierter Spezialist für Airbags, ABS und Sicherheitsgurte in der IT. Zehn IT-Sicherheitsexperten mit 70 Mannjahren Erfahrung beraten, entwickeln und implementieren IT-Lösungen für Kunden weltweit. Der Fokus liegt dabei auf Themen wie Prozess-Optimierung und Security-Management. Risiko-Analyse, die Sicherheitsberatung, Auditing, Security-Leitfäden, Software-Entwicklung, Reporting bis zum Training.

www.secadm.de

SecureNet GmbH, München

Als Softwarehaus und Web Application Security Spezialist bieten wir Expertise rund um die Sicherheit von Webanwendungen: Anwendungs-Pentests, Sourcecodeanalysen, Secure Coding Guidelines, Beratung rund um den Software Develoment Lifecycle. Tools: Application Firewalls, Application Scanner, Fortify SCA/Defender/Tracer.

www.securenet.de

underground_8
secure computing gmbh

Wir entwickeln und vertreiben security appliances für die Bereiche Unified Threat Management, Traffic Shaping und Antispam. Unsere Lösungen sind hardwarebasiert und werden über Distributoren, Reseller und Systemintegratoren implementiert und vertrieben.

www.underground8.com