itsecurity

itsecurity

Ausgabe 5-6 2010 www.it-daily.net € 20,-

Titel

Gibt es Sicherheit in Social Networks?

Management

Einsatz von IT-GRC-Plattformen am Beispiel IT-Risikomanagement

Produkt & Praxis

Zurück in die Zukunft Next Generation Firewalling

Triple Biometry eXtreme Security dank Prozess-Parallelität

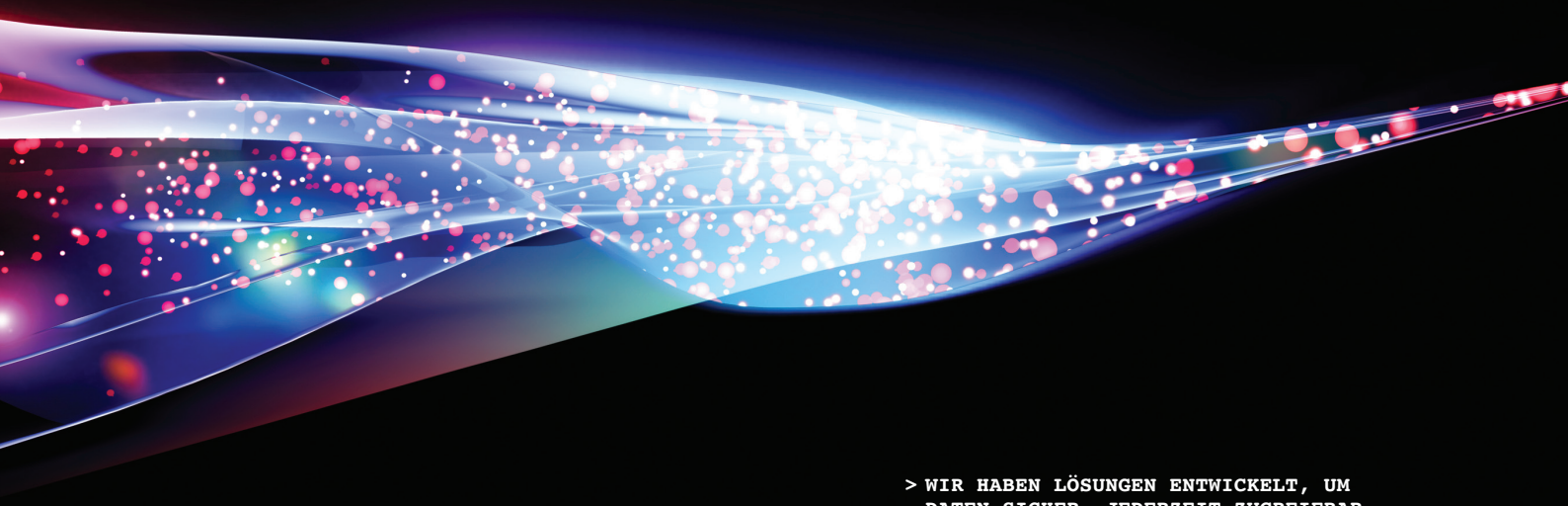
Service

Vorgehensmodell für den Datenschutz bei Offshoring-Projekten

itverlag

> WENN IHRE INFORMATIONS-ÜBERMITTLUNG STOPPT WÄRE DAS EIN STILLSTAND FÜR IHR UNTERNEHMEN

> GUT, DASS WIR DANN DA SIND



> WIR HABEN LÖSUNGEN ENTWICKELT, UM DATEN SICHER, JEDERZEIT ZUGREIFBAR UND ZUVERLÄSSIG ZU VERSENDEN

> WENN E-MAILS, WEBZUGRIFFE ODER IHR INSTANT MESSENGER BEDROHT SIND – SCHÜTZEN WIR SIE

> WENN E-MAILS UND INSTANT MESSENGER NACHRICHTEN ABGELEGT WERDEN SOLLEN – ARCHIVIEREN WIR DIESE FÜR SIE

> WENN NACHRICHTEN NICHT FÜR DRITTE LESBAR SEIN SOLLEN – DANN VERSCHLÜSSELN WIR DIESE

> WENN IHR E-MAIL SYSTEM AUSFÄLLT – SORGEN WIR DAFÜR, DASS ES TROTZDEM WEITERGEHT

> WAS IMMER SIE FÜR IHR BUSINESS BRAUCHEN – WIR HABEN DIE LÖSUNG FÜR EINE ZUVERLÄSSIGE KOMMUNIKATION. ZUSÄTZLICH BIETEN WIR MEHRSPRACHIGEN SUPPORT AN 24 STUNDEN, 7 TAGE DIE WOCHE. DAS IST EIN WIRKLICHER SERVICEGEDANKE – AUCH WENN WIR ES SELBST BEHAUPTEN..

FÜR MEHR INFORMATION RUND UM UNSERE SERVICEDIENSTE UND LÖSUNGEN, BESUCHEN SIE UNSERE WEBSEITE: WWW.MESSAGELABS.DE/PRODUCTS

MessageLabs
SYMANTEC HOSTED SERVICES™

Confidence in a connected world. symantec™

Ulrich Parthier,
Publisher
itsecurity

Cloud Computing und die IT-Sicherheit

Das Thema Cloud Computing hat in den letzten Monaten enorm an Bedeutung gewonnen.

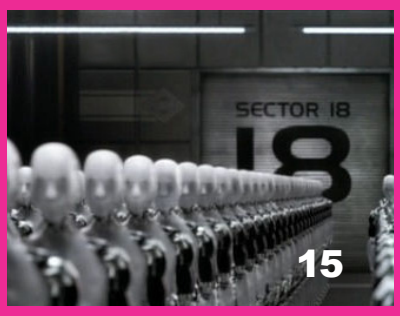
Es stellt die Anwender jedoch vor eine im Vergleich zu anderen Formen des „Outsourcing“ wesentlich veränderte Situation. Erstens werden aufgrund der gemeinsamen Nutzung von Plattformen (ICT), der Verteilung der Systeme und der Bereitstellung etwa über das Internet, die Fragen nach Sicherheit bzw. nach entstehenden Risiken augenfällig. Dazu kommt, dass der Anbieter häufig IT- und TK-Leistungen in komplexer Art und Weise zusammenführt. Es entstehen also neue und veränderte Bedrohungen auf die Sicherheit. Zweitens sind das ad-hoc Wissen und die Einflussmöglichkeiten des Anwenders beschränkt. Gerade öffentliche Wolken sind intransparent, für den Anwender nicht einsehbar, und werden dem Anwender als „Fertigprodukt“ mit wenigen Variationsmöglichkeiten zum Abonnement angeboten.

Interner Druck kommt auch aus den Unternehmen selbst. Da diese ihre IT heute und in den kommenden Jahren verstärkt konsolidieren müssen, werden sie zunehmend auf Cloud Computing setzen. Damit steigt auch die Nachfrage nach virtualisierten Infrastrukturen, egal ob intern oder beim IT-Dienstleister. Unternehmen profitieren in vielerlei Hinsicht, wenn sie skalierbare Sicherheits- und Managementlösungen als virtualisierte Appliances einsetzen: die Kosten sind geringer, die Kapazitäten der Infrastruktur werden besser ausgeschöpft, gleichzeitig vereinfacht sich das Management – Verfügbarkeit, Effizienz und Stabilität steigen.

Doch wie geht man vor? Eine Checkliste hilft, die Sicherheitsaspekte fest im Blick zu behalten:

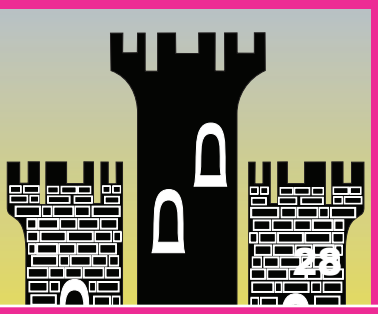
1. Zugriffskontrolle, Verwaltung von Identitäten mit Rollen und Rechten, Sicherheit auf Nutzerseite
2. Sichere Kommunikation in die Cloud
3. Trennung von Daten und Anwendungen verschiedener Nutzer (Mandanten)
4. Sichere Kommunikation innerhalb der Cloud
5. Absicherung von IT-Systemen, Plattformen und Anwendungen (IT-Sicherheit)
6. bauliche und physische Sicherheitsmaßnahmen (RZ-Sicherheit)
7. Personal und Sicherheitsorganisation (Ressourcen, Qualifikation, Überprüfungen)
8. Business Continuity Management, Backup und Desaster Recovery
9. Verträge, SLA, Service Management, Reporting, Integration in Prozesslandschaften des Nutzers
10. Security Management, Richtlinien, Organisation
11. Incident Management (ICT-Dienstleister und Nutzer)
12. Anforderungsmanagement, Compliance, Datenschutz

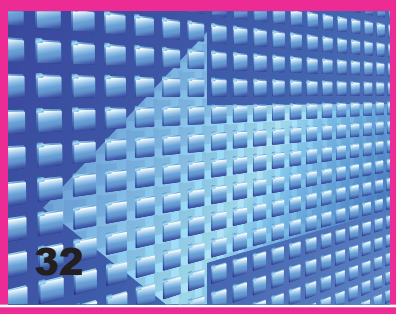
Quelle: T-Systems



Inhalts-verzeichnis

Ausgabe 5-6/2010





Inserentenverzeichnis

Vasco Identikey Server Banking Edition

Vasco (www.vasco.com) Anbieter von Sicherheitslösungen und Spezialist für Authentifizierung, erweitert die Möglichkeiten seines Servers IDENTIKEY. Die neue Banking Edition unterstützt auch Authentifizierung auf Basis von EMV-CAP oder Hardware Security Module (HSM).

Die Identikey Server Banking Edition wird standardmäßig Virtual Digipass bieten. Dabei handelt es sich um eine anwenderfreundliche Lösung für Strong User Authentication und digitale Signatur. Der Kunde gibt auf der Banking-Site zunächst Usernamen und PIN ein. Dann sendet die Bank per SMS ein Einmalpasswort an das Handy des Kunden. Dieser empfangene Code gibt den Zugang zur Banking-Applikation für den Anwender frei.

www.vasco.com

GFI Software bringt Backup-Lösung

GFI Software hat eine Backup-Lösung vorgestellt, die speziell auf kleine und mittlere Unternehmen zugeschnitten ist. GFI Backup 2010 - Business Edition eignet sich für IT-Administratoren, die mit einem einzigen Backup- bzw. Restore-Task ein komplettes Netzwerk absichern wollen. Dies ermöglicht nicht nur eine schnellere Konfiguration des Backups, sondern erspart auch jedes Mal multiple Änderungen, wenn sich die Policies für die Datensicherung ändern. Spezielles Augenmerk wurde bei der Entwicklung darauf gelegt, dass der Restore-Prozess zuverlässig, effizient, schnell und einfach zu verwalten ist.

www.gfisoftware.de

Vierergespann für Sicherheit und Management

Symantec präsentiert neue Lösungen, um Internetbedrohungen die Stirn zu bieten: Mit den Suiten Control Compliance Suite 10.0, Data Loss Prevention Suite 10.5, Altiris IT Management Suite 7.0 und Symantec Protection Suites unterstützt Symantec Sicherheit und Verwaltung von Unternehmens-IT. Die Erfahrungen des Symantec Global Intelligence Networks haben gezeigt, dass Geschäftsumgebungen bei folgenden Faktoren zum besonderen Ziel für Angreifer werden: unzusammenhängenden IT-Richtlinien, ungenügend geschützte Informationen sowie schlecht gemanagte Systeme und vernachlässigte Infrastruktur.

www.symantec.com

Gemalto Smart Guardian
wahrt Integrität mobiler Daten

LWP gibt die Verfügbarkeit des Protiva Smart Guardian bekannt. Das von Gemalto, einem führenden Anbieter von digitalen Sicherheitslösungen, entwickelte Gerät basiert auf Smart-Card-Technologie und schützt die auf dem USB-Stick verschlüsselt gespeicherten Daten nach höchsten Standards vor nicht autorisiertem Zugriff. Damit gewährleisten Unternehmen die Integrität ihrer mobilen Daten und vermeiden finanzielle Schäden und Wettbewerbsnachteile.

Er bietet mobilen Arbeitnehmern, die einen Großteil ihrer Aufgaben unterwegs erledigen, eine vertrauenswürdige Plattform für den sicheren Zugriff auf Unternehmensdaten. Dabei verbindet der Smart Guardian die Endpunktkontrolle mit der sicheren Speicherung und schützt auf diese Weise sensible Daten. Die neue Lösung garantiert ein besonders hohes Sicherheitsniveau, da die verschlüsselten Daten den Smart Guardian nie verlassen. Entdeckt das System Manipulationsversuche beziehungsweise einen Eindringversuch, werden alle Daten auf dem Token gelöscht. Darüber hinaus lässt sich Smart Guardian sehr einfach und bequem handhaben. Um das Gerät zu entsperren, muss der Anwender lediglich seinen registrierten, mobilen Token einstecken und ein Passwort eingeben. Alle auf das Gerät übertragenen Daten werden dann automatisch verschlüsselt.

Smart Guardian bietet eine Zwei-Faktoren-Authentifizierung, die auf den Komponenten Besitz und Wissen basiert: Der Zugriff ist nur mit USB-Token und persönlichem Passwort möglich. Damit stellt Gemalto sicher, dass nur berechtigte Anwender auf die verschlüsselten Daten zugreifen können, selbst wenn das Gerät verloren geht oder gestohlen wird. IT-Administratoren können die Smart Guardian-Token problemlos einsetzen und verwalten; Anwender benötigen keine Schulung. Der Token kombiniert die erprobte, sichere Smart Card-Technologie von Gemalto mit der sicheren Flash-Technologie von Lexar.

Über die Verwaltungsoptionen können Endnutzer und Administratoren neue Geräte ganz einfach registrieren, Software-Aktualisierungen durchführen oder geschützte Unternehmensanwendungen zum Einsatz bringen. Zudem kann man verlorene oder gestohlene Token aus der Ferne sperren und alle auf ihnen gespeicherten Daten löschen.

www.lwp.de

Spike Licensing: Lizenzen für den Notfall

Wolke per Fernzugriff: Mit seiner neuen virtuellen StoneGate SSL VPN Appliance sowie der Software SSL VPN 1.4 und der Appliance SSL-1060 ermöglicht Stonesoft einen sicheren Zugriff auf Daten und Anwendungen in der Cloud – sowohl von mobilen Geräten aus als auch über Remote-Verbindungen. Die neuen Lösungen erweitern das Stonesoft-Portfolio für sicheren Netzwerkzugriff in virtuellen Umgebungen. Mit StoneGate SSL VPN können Unternehmen ihren Mitarbeitern, Partnern oder Kunden schnell und einfach einen flexiblen Remote-Zugriff auf ihre Daten bereitstellen. Gleichzeitig haben sie immer die umfassende Kontrolle darüber, wer wann und von welchem Ort aus auf ihr Netzwerk zugreift. Die virtuelle StoneGate SSL VPN Appliance, SSL VPN 1.4 und SSL-1060 sind ab sofort verfügbar.

Alle SSL-VPN-Appliances von Stonesoft unterstützen ab sofort auch Spike Licensing. Mit diesen temporären Lizenzen lässt sich in Ausnahmesituationen die Nutzerzahl kurzfristig erhöhen. Zum Beispiel, wenn – wie im Fall der Schweinegrippe – plötzlich viele Mitarbeiter von zu Hause aus arbeiten oder das Firmengebäude beispielsweise aufgrund eines Wasserschadens nicht genutzt werden kann. In solchen Fällen kann die Möglichkeit, die Anzahl der Remote-Nutzer innerhalb kurzer Zeit zu erhöhen, ein unternehmenskritischer Faktor sein.

„Der sichere Zugriff auf Unternehmensdaten von unterwegs oder vom Home Office aus ist mittlerweile kein Luxus mehr. In der sich immer rasanter entwickelnden Geschäftswelt ist er zu einer Notwendigkeit geworden, die über Erfolg und Misserfolg eines Unternehmens entscheiden kann. Die neue StoneGate SSL VPN Appliance hilft Unternehmen, ihre Prozesse zu optimieren, und bietet Tools für neue Geschäftsmöglichkeiten – ohne Kompromisse bei der Sicherheit“, sagt Hermann Klein, Country Manager DACH bei Stonesoft.

„Wenn lokale und mobile Nutzer, Mitarbeiter im Home Office, Partner, Lieferanten oder andere Anwender Zugriff auf Daten und Applikationen erhalten sollen, spielt die Authentifizierung eine zentrale Rolle. Leider wird diesem Thema oft zu wenig Aufmerksamkeit gewidmet. Authentifizierung ist weitaus mehr als nur das Anlegen eines Benutzernamens und eines Passworts. Deshalb sollten Unternehmen die Integration bestehender Authentifizierungssysteme sorgfältig planen“, so Klein weiter.

www.stonesoft.de.

Fünf Wege,
um die virtuelle Netzwerksicherheit zu erhöhen

Stonesoft zeigt fünf Wege, mit denen Unternehmen die Sicherheit in ihrer Cloud verbessern können. Viele Firmen haben es versäumt, bei der Planung ihrer Virtualisierungsprojekte auch die Informations- und Sicherheitsverantwortlichen von Anfang an mit einzubeziehen.

Stattdessen haben sie ihre virtuellen Netzwerke einfach nur in die bestehenden, auf physikalische Netzwerke zugeschnittenen, Sicherheits-Strategien und -Technologien integriert. Diese kurzsichtige Herangehensweise kann die gesamte Netzwerksicherheit gefährden. Dies ist für Unternehmen eine der größten Herausforderungen auf dem Weg zu erfolgreichem Cloud Computing.

Mithilfe der folgenden fünf Tipps von Stonesoft, Anbieter integrierter Lösungen für Netzwerksicherheit und Business Continuity, können sich IT-Verantwortliche gegen Sicherheitsbedrohungen und -attacken in der Cloud schützen und den Erfolg ihrer Cloud-Computing-Strategien sicherstellen:

1 Föderierte Identitäten (Federated ID):

In einer Cloud-Computing-Umgebung müssen sich Mitarbeiter bei mehreren Anwendungen und Diensten anmelden können. Dies kann zu einer erheblichen Sicherheitsfalle werden, wenn Unternehmen eine starke Authentifizierung auf Anwenderebene nicht gewährleisten können. Um dieses Risiko abzufedern, sind „Single-Sign-on"-Funktionen (SSO) erforderlich, wie sie beispielsweise die Appliance StoneGate SSL VPN bereitstellt. Damit können Anwender mit nur einem Login auf mehrere Anwendungen und Dienste zugreifen – auch in der öffentlichen Cloud außerhalb des Unternehmens. Mithilfe von SSO können Unternehmen ihr Sicherheitsmanagement optimieren und eine starke Authentifizierung innerhalb der Cloud sicherstellen.

2 Unterbrechungsfreie Konnektivität:

Ist ein Großteil der kritischen Unternehmensdaten in der Cloud gespeichert, kann ein Netzwerkausfall den gesamten Geschäftsbetrieb gefährden. Der Zugriff auf Cloud-Dienste muss daher jederzeit gewährleistet sein, auch während einer Wartung. Dies erfordert innerhalb der Netzwerkinfrastruktur Hochverfügbarkeitstechnologien und -funktionen wie Active/Active-Clustering, Dynamic Server Load Balancing und ISP Load Balancing. Dabei sollten Unternehmen Technologien verwenden, die bereits in ihre Netzwerklösungen integriert sind, anstatt sie als Einzelprodukte zu kaufen. Nur so lassen sich Effektivität und Benutzerfreundlichkeit sowie geringere Netzwerkkosten sicherstellen.

3 Multi-Layer-Kontrolle:

Die zunehmende Verbreitung von Cloud-Computing-Umgebungen und immer komplexere Sicherheitsbedrohungen erfordern innerhalb des Netzwerks ein mehrschichtiges Abwehrsystem, bestehend aus Schutzmechanismen am Netzwerkrand und IDP-Funktionen (Intrusion Detection and Prevention). Anstatt Firewalls der ersten Generation als Perimeterschutz in der Cloud zu implementieren, empfiehlt Stonesoft den Einsatz virtueller Firewall-Appliances der nächsten Generation wie die StoneGate Virtual NextGen Firewall. Diese bieten erweiterte Firewall- und IPS-Funktionen für eine umfassende Analyse des Datenverkehrs (Deep Traffic Inspection). Dadurch können IT-Verantwortliche jede Art von Datenverkehr überwachen – von einfachem Webbrowsing über Peer-to-Peer-Anwendungen bis hin zu verschlüsseltem Web-Datenverkehr in einem SSL-Tunnel. Zusätzlich sollten Unternehmen weitere IPS-Appliances implementieren, um ihr Netzwerk vor internen Attacken zu schützen, die den Zugriff auf die Cloud bedrohen könnten.

4 Zentrales Management:

Menschliche Fehler stellen immer noch die größte Sicherheitsbedrohung dar, sowohl in physikalischen als auch in virtuellen Umgebungen. Dieses Risiko steigt exponentiell, je mehr Geräte ein Unternehmen zur Sicherung seiner virtuellen Netzwerke zusätzlich einsetzt. Denn dadurch werden das Management, die Überwachung und Konfiguration von Netzwerken immer komplexer und unstrukturierter. Deshalb empfiehlt Stonesoft eine zentrale Management-Konsole zur Verwaltung, Überwachung und Konfiguration von allen physikalischen und virtuellen Geräten sowie Drittanbieter-Produkten.

5 Virtueller Desktop-Schutz:

Immer mehr Unternehmen setzen auf Desktop-Virtualisierung, um von dem Kostenvorteil und der einfachen Administration zu profitieren. Diese virtuellen PCs sind jedoch mindestens genauso anfällig für Sicherheitsbedrohungen wie physikalische Computer – wenn nicht sogar anfälliger. Um sie ausreichend zu schützen, sollten Unternehmen sie von anderen Netzwerkbereichen isolieren und Deep Inspection auf Netzwerkebene implementieren. So lassen sich sowohl interne als auch externe Bedrohungen abwehren. In Sachen Sicherheit sollten Unternehmen einen mehrschichtigen Ansatz verfolgen: Mit IPS-Technologie (Intrusion Prevention System) können sie unbefugte Zugriffe innerhalb des Netzwerks verhindern und Clients vor bösartigen Servern schützen, während zusätzlich IPsec- oder SSL VPN-Technologien unbefugte Zugriffe von außen abblocken und sicheren Fernzugriff auf Anwendungen bereitstellen.

www.stonesoft.com

Neue Gefahren in Unternehmen

Gibt es Sicherheit in Social Networks?

Analysiert man ganz allgemein Verursacher und Art von Sicherheitsvorkommnissen in den letzten Jahren, so lassen sich einige interessante Tendenzen recht schnell ermitteln.

Die Angreifer arbeiten mittlerweile deutlich professioneller, sind besser organisiert und gehören nicht selten kriminellen Organisationen an. Demzufolge hat sich auch die Zielrichtung der Angriffe verlagert: weg von aufsehenerregenden Einzelaktionen hin zu finanziell lukrativen Aktivitäten. Deshalb hat der Aufbau von weltweiten Bot-Netzen mit der Möglichkeit Massenangriffe zu starten ebenso zugenommen wie der Diebstahl von Firmengeheimnissen oder der Identitätsdiebstahl. Letzterer spielt eine zunehmende Rolle bei den immens steigenden Angriffen auf sog. Social Networks wie etwa Twitter, Facebook oder Xing. Nachstehend soll deshalb die Entwicklung dieser Social Networks aufgezeigt und unter Sicherheitssicht bewertet werden.

Nachdem in den ersten Jahren der weltweit wachsenden Internet-Nutzung noch vorwiegend altbekannte Online-Portale wie AOL oder Yahoo zum Aufbau von User-Communities genutzt wurden, haben in den letzten Jahren zunehmend die „Social Networks“ das Feld übernommen. Das social networking ist mittlerweile wohl eine der populärsten Aktivitäten im Internet mit einer geschätzten Anzahl von aktuell mehreren hundert Millionen Nutzern und einer täglichen Zuwachsrate von weit über einer Million Neuanmeldungen. Allein der Branchenführer Facebook meldet über 400 Millionen aktive Nutzer (Stand: 02/2010) aus 180 Ländern, von denen täglich mehr als 50% online sind.

Der Reiz

Was macht nun den Reiz dieser Social Networks aus? Auf der Webtechnologie basierend sind sie nichts anderes als Online Communities, die es den Teilnehmern ermöglichen, sich mit anderen Teilnehmern innerhalb vorgegebener Funktionalitäten auszutauschen. Wesentlicher Bestandteil eines Social Networks ist das Anlegen von spezifischen Nutzer-Profilen mit persönlichen Informationen, benannten Freunden (mit erweiterten Möglichkeiten zur Kommunikation) und Gruppen (Nutzer mit gleichen Interessen). Ob jetzt Photos und Videos ausgetauscht werden, Online-Verabredungen getroffen werden oder über Gott-und-die-Welt diskutiert wird, bleibt den Möglichkeiten des Networks und den Intentionen der Nutzer überlassen.

Gerade die jüngere Generation ist in den Social Networks besonders aktiv vertreten, in den USA etwa geht man von über 80% Nutzern unter Studenten aus. Aber auch in Deutschland beschäftigt das social networking

nicht nur die Jugend in Facebook, SchülerVZ oder StudiVZ, mittlerweile werden eine Vielzahl von geschäftlichen Kontakten auch über Xing oder LinkedIn geknüpft. Und zur schnellsten Informationsquelle über nahezu alle Ereignisse, die weltweit gerade stattfinden, hat sich Twitter gemausert. Die bereits jetzt überaus hohe Nutzung der Social Networks, verbunden mit den zu erwartenden starken Zuwachsraten, ist schon lange keine reine Privatangelegenheit mehr, sondern zwingt mittlerweile auch die Unternehmen, sich ernsthaft mit dieser Entwicklung zu beschäftigen. Viele Nutzer werden ihren Online-Aktivitäten eben nicht nur im Privatbereich nachgehen, sondern erfahrungsgemäß dies auch während der Arbeitszeit nicht unterlassen. Deshalb ziehen es immer mehr Unternehmen in Betracht, den Zugriff auf Social Networks während der Arbeitszeiten sogar ganz zu sperren. Der Grund dafür ist nicht nur die Angst vor deutlichen Produktivitätseinbußen, sondern zunehmend kommen auch Sicherheitsbedenken ins Spiel. Diverse Untersuchungen belegen, wie lax die Nutzer mit dem Thema Sicherheit umgehen. So ergab die kürzlich vorgestellte Studie „Bringing Social Security to the Online Community" des CMO Council [1] teilweise erschreckende Ergebnisse:

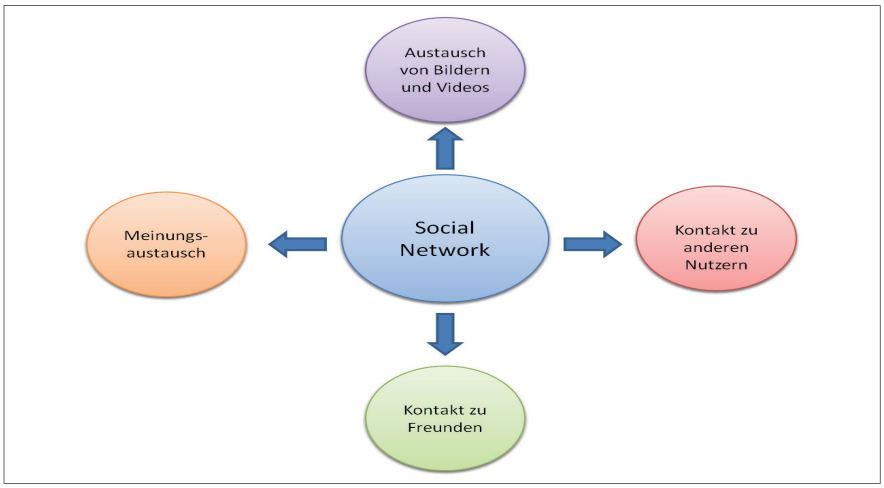


Bild 1: Typische Angebote von Social Networks.

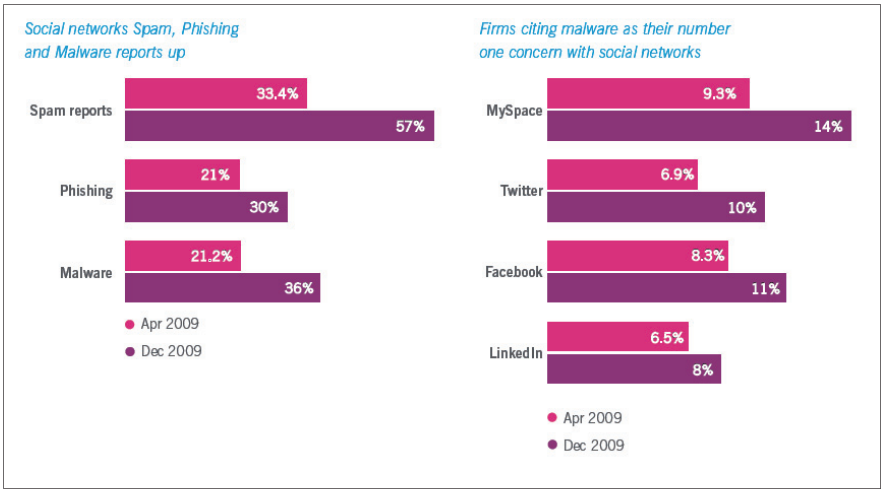


Bild 2: Angriffe auf Social Networks [2].

- Weniger als 1/3 der Nutzer treffen überhaupt Sicherheitsvorkehrungen
- 21 % akzeptieren Kontaktanfragen von Fremden
- 64% folgen empfohlenen Web-Links bedenkenlos
- 26% tauschen Dateien innerhalb des Social Networks aus
- 64% ändern nie ihr Passwort
- aber
- 20% hatten schon mit Identitätsdiebstahl zu tun
- 47% waren schon Opfer eingeschleppter Malware
- 55% hatten mit Phishing-Attacken zu tun

Wegen dieser Nachlässigkeiten besteht die wohl begründete Angst, dass Mitarbeiter Aussagen tätigen und Fotos oder Videos veröffentlichen, die für das Unternehmen schädlich sein könnten. Obwohl Social Networks wie Facebook auch für legitime Geschäftszwecke verwendet werden können, sollten die IT-Verantwortlichen die Entscheidungsgewalt darüber haben, ob der Zugriff darauf für Mitarbeiter ihres Unternehmens angebracht ist oder nicht.

Gerade die zunehmenden Probleme durch Identitätsdiebstahl, Einschleppen von Malware, Datenverlust und Reputationsrisiken für das Unternehmen spielen dabei eine gewichtige Rolle.

Wie steht es mit der Sicherheit?

Insbesondere von den größeren Social Networks wie Facebook, MySpace, LinkedIn oder Twitter ist bekannt, dass sie seit 2009 zunehmenden Spam- und Malware-Attacken ausgesetzt sind. All diese zielten in erster Linie darauf ab, die Nutzer-PCs zu kompromittieren und sensible Informationen zu stehlen.

Der Sophos Security Threat Report 2010 [2] belegt, daß nicht nur das Spammen deutlich zugenommen hat, sondern daß auch die Versuche Usernamen und Passworte der Nutzer zu ermitteln deutlich angestiegen sind.

Diese Art des Identitätsdiebstahls ist relativ leicht umzusetzen, da viele Nutzer sehr lax mit ihren Zugangsdaten umgehen und entweder nur schwache (=erratbare) Passwörter verwenden oder aber sich diese Daten leicht entlocken lassen. Sind Nutzer-Accounts erst einmal gehackt, dann bieten sich dem Angreifer vielfältige Möglichkeiten, unter dieser Identität an deren Freunde und Bekannte erneut Spam oder Malware zu versenden. Diese scheint den Empfängern dann aus vertrauenswürdiger Quelle zu kommen und lässt sie schnell alle üblichen Vorsichtsmaßnahmen vergessen, mit dem Ergebnis, dass sie selber kompromittiert werden.

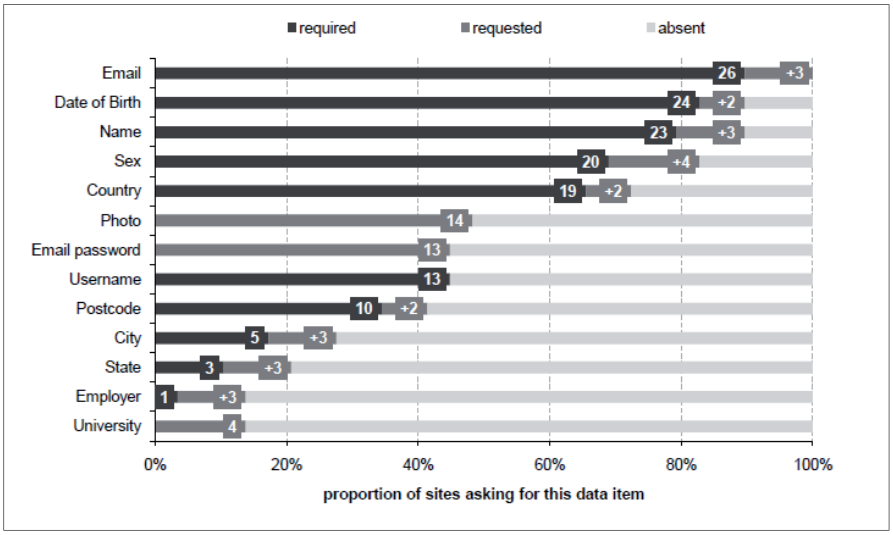


Bild 3: Abgefragte Daten zum Nutzer-Profil [3].

visibility level	default	optional	unavailable
public Internet	41%	-	59%
all site users	48%	28%	24%
sub-networks only	7%	17%	76%
friends of friends	-	24%	76%
friends only	3%	79%	17%

Tabelle 1: Sichtbarkeit der gesammelten Daten [3].

Mittlerweile können diese Angriffe auch weitgehend automatisiert ablaufen. So konnte der Koobface-Wurm selbstständig einen Facebook-Account anlegen, diesen per E-Mail bestätigen, sich in Gruppen anmelden und Kontakt-Messages an andere Nutzer versenden.
Bereits über 100 Millionen Nutzer setzen mittlerweile auch intelligente Mobilgeräte (Handys, Smartphones, Netbooks) für den Zugang zu Social Networks ein.

Nicht selten wird das verwendete Mobilgerät auch als Backup-Gerät für Geschäftsmails, persönliche Daten, Kontaktangaben, Bilder und Zugangscodes genutzt.

Ein verlorenes oder gestohlenes Gerät könnte unabsehbare Konsequenzen für den kompromittierten Nutzer und seine Privatsphäre haben. Sind mit so einem gestohlenen Account dann sogar Zugriffe auf unternehmensrelevante Daten möglich, dann sind natürlich auch Unternehmensbelange gravierend berührt. Dieser

Site	Data Collection Score	Privacy Control Score	Privacy Policy Score	**Privacy Score**	Functionality Score
LinkedIn	0.52	0.39	0.67	**0.70**	0.50
meinVZ	0.38	0.41	0.65	**0.65**	0.40
Facebook	0.10	0.61	0.41	**0.53**	0.90
Xing	0.24	0.37	0.57	**0.52**	0.30
Twitter	0.81	0.26	0.30	**0.49**	0.10
MySpace	0.29	0.41	0.43	**0.48**	0.80
Kaioo	0.57	0.15	0.46	**0.43**	0.20

Anmerkung: Die Scores wurden normalisiert; höherer Wert = besseres Ergebnis.

Tabelle 2: Analyse-Ergebnisse zur Bewertung von Privacy / Functionality (Auszug aus [3]).

Risiken sind sich aber viele Nutzer überhaupt nicht bewusst.

Social Networks unter der Lupe

Eine umfangreiche Analyse zum Thema Sicherheit in Social Networks legt „The Privacy Jungle: On the Market for Data Protection in Social Networks“ [3] vor. Insbesondere die Behandlung des Schutzes der Privatsphäre wurde bei 45 Social Networks unter Bewertung von 260 unterschiedlichen Kriterien weltweit untersucht. Gerade der intensive Kampf um neue Nutzer führt zumindest bei einigen Betreibern zu einer starken Aufweichung aller Sicherheitsbedenken. Durch den wettbewerbsbedingten Druck, immer neue Funktionalitäten innerhalb der Social Networks anzubieten, kommen Sicherheitsbelange häufig zu kurz.

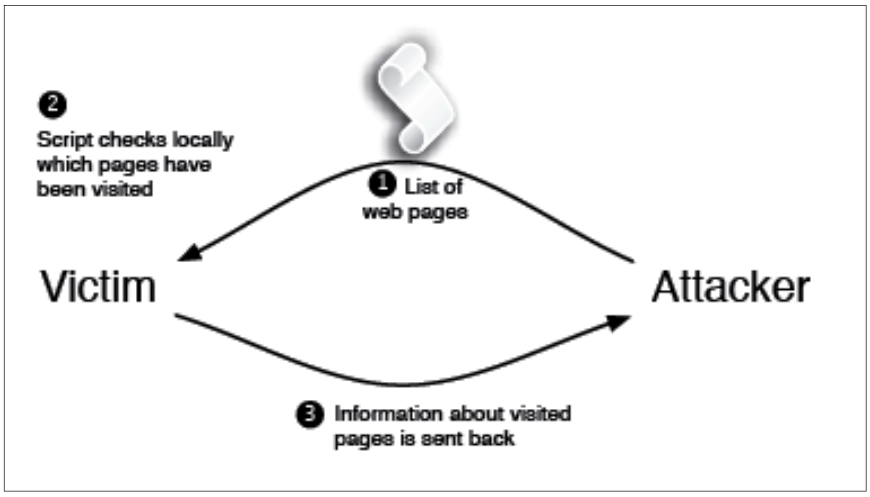


Bild 4: Technik des „History Stealing“ [4].

Auffällig war bei der Analyse besonders die Menge an privaten Informationen, die von den Social Networks abgefragt werden.

Diese privaten Daten werden, von den Nutzern aus Bequemlichkeit oder ganz einfach aus Unwissenheit nur unzureichend geschützt. Noch schlimmer aber ist, dass einige der Social Networks sogar per Default diese Daten im gesamten Internet jedem zugänglich machen. Was man damit unter anderem anstellen kann wird später noch aufgezeigt.

Des Weiteren werden all diese Daten auch nicht unbedingt benötigt, um die Funktionalitäten im Social Network aufrecht zu erhalten. Da die Teilnahme häufig kostenfrei oder zumindest vergleichsweise günstig ist, darf man wohl davon ausgehen, dass die Betreiber andere Einnahmequellen ins Auge gefasst haben. So dürften viele der abgefragten Nutzerdaten

	Facebook	MySpace	Friendster	LinkedIn	StudiVZ	Xing	Bigadda	Kiwibox
Uses dynamic links	✔	✔	✔	✔	✔	✔	✔	✔
Group directory	Full	Searchable	Full	Searchable	Searchable	Searchable	Searchable	Full
Member directory	Full	Searchable	Full	Full	Searchable	Searchable	Searchable	Searchable
Group member enumeration	≤6,000	Unlimited	Unlimited	≤500	Unlimited	Unlimited	Unlimited	Unlimited
Public member profiles	✔	✔	✔	✔	✔	✔	✔	×
Vulnerable	✔	✔	✔	✔	✔	✔	✔	✔

Tabelle 3: Chancen zur De-Anonymisierung mittels weiterer Social Networks [4].

sicherlich auch für die kommerzielle Nutzung durch andere Marktteilnehmer interessant sein. So trat Facebook zuletzt mit nur unzulänglich verhüllten Begehrlichkeiten in Erscheinung und gab die geplante Änderung der Allgemeinen Geschäftsbedingungen bekannt, die eine weitere Lockerung des Datenschutzes mit sich bringen würde. Besonders die Weitergabe von persönlichen Profilinformationen stieß allerorten übel auf und rief vehemente Nutzerproteste hervor.

Die Analyse zur Umsetzung der Anforderungen an eine Privacy Policy ergab weiterhin eine Vielzahl von nicht implementierten oder nicht korrekt umgesetzten Funktionen (Details sind [3] zu entnehmen). Gebildet aus diesen Ergebnissen und einer zusätzlichen Bewertung der im Network gesammelten Daten und der hierfür den Nutzern zur Verfügung stehenden Kontrollfunktionen wurde ein Privacy Score ermittelt, der zu einem Ranking der untersuchten Social Networks führte. Zusätzlich wurde auch die jeweils angebotene Funktionalität bewertet, um festzustellen, ob sich eine Korrelation zwischen Privatheit und Funktionalität herstellen lässt.

Der Auszug in Tabelle 2 zeigt einige der in Deutschland stärker frequentierten Networks mit ihrem Ranking. Insgesamt liegt der ermittelte Privacy Score zwischen 0.70 und 0.26.

Fragwürdige Anonymität

Wer meint, sich im Internet nahezu anonym zu bewegen, dem könnte seine Mitgliedschaft in einem Social Network eine große Überraschung bescheren. Durch die dort freiwillig gemachten Angaben lassen sich Rückschlüsse auf die Identität eines Nutzes auch außerhalb des Social Networks ziehen, also nix mehr mit Anonymität. Die hierzu von Forschern des Isec-Forschungslabors für IT-Sicherheit entwickelte De-Anonymisierungssoftware nutzte in erfolgreichen Tests die in Deutschland stark verbreitete Business-Plattform Xing, auf der mehrere Millionen Anwender ihre Profile veröffentlichen.

Im Wesentlichen macht sich der Test zunutze, dass viele Xing-Nutzer über ihre Zugehörigkeit zu mehreren unterschiedlichen Gruppen mit einer gewissen Wahrscheinlichkeit identifizierbar sind. Es gibt nur wenige Personen in solch einem großen sozialen Netz, die exakt den gleichen Gruppen angehören. Um an die für die Identifizierung benötigten Informationen zu gelangen muss man möglichst viele Gruppen in Xing und die dazugehörigen Foren durchsuchen, dies ist aber relativ unproblematisch, da der Zugang praktisch ungeschützt ist. Im Test wurden rund 1,8 Millionen Nutzer gefunden, die in etwa 7.000 Gruppen organisiert waren. Aus diesen öffentlich zugänglichen Informationen wurde eine Datenbank der Gruppenzugehörigkeiten erzeugt.

Danach begann der eigentliche Deanonymisierungstest. Es wurde eine Art „Fingerabdruck“ des Browsers erstellt, an dem der zu identifizierende Nutzer saß. Hierzu bediente man sich des sog. «History Stealings», eine Technik die es ermöglicht, die von einem Browser in der Vergangenheit besuchten Links auch von Ferne zu ermitteln. Damit konnte nun festgestellt werden, welche Gruppenseiten (=Links) im anvisierten Social Network dieser Nutzer besucht hatte. Im Abgleich mit der o.g. Datenbank ergab sich dann mit einer ansprechenden

Wahrscheinlichkeit die gesuchte wahre Identität des Nutzers.

Die Grundlagen des Tests haben die Autoren Gilbert Wondracek, Thorsten Holz, Engin Kirda und Christopher Krügel im Dokument «A Practical Attack to De-Anonymize Social Network Users» [4] vollständig beschrieben. Darin schlagen sie auch Abhilfemaßnahmen zum Schutz vor solchen Deanonymisierungsangriffen vor. Alle Maßnahmen sehen vor, das History Stealing zu erschweren. Auf Server-Seite könnten die Betreiber randomisierte Token in die URLs einfügen, die das spätere Durchprobieren dieser URLs erheblich erschweren würde. Auf Client-Seite hilft es, den Zugriff auf die Browser-History zu verwehren, beispielsweise indem man bestimmte Seiten nur im Inkognito-Mode aktueller Browser ansurft, zusätzliche Schutz-Plug-ins wie NoScript für den Firefox verwendet oder regelmäßig die History löscht. Es soll aber auch nicht unerwähnt bleiben, dass die Betreiber von Xing nach Bekanntwerden dieser Vorgehensweise sehr schnell reagierten und dies serverseitig unterbanden. Die Autoren haben neben Xing auch weitere Social Networks überprüft und gehen bei diesen von ähnlichen Möglichkeiten der De-Anonymisierung aus.

Was ist zu tun?

Es bleibt festzustellen, dass das immense Wachstum der Social Networks die verfügbaren Sicherheitsmaßnahmen und Vorkehrungen zum Schutz der privaten Informationen deutlich überfordert. Hinzu kommt der unvorsichtige Umgang der meisten Nutzer mit den ihnen angebotenen Möglichkeiten innerhalb der Networks. Ist das für den einzelnen Nutzer schon mit Risiken verbunden, dann stellt die Nutzung am Arbeitsplatz durchaus ein beachtenswertes Sicherheitsrisiko dar. Einige Unternehmen sind bereits dazu übergegangen, den Zugang zu Social Networks gänzlich für ihre Mitarbeiter zu sperren. Hierfür gibt es die bekannten Anbieter von Lösungen zur Content-Filterung, denn das Einschränken von Zugriffen auf bestimmte Websites ist ja kein wirklich neues Thema.

Ebenso wenig neu ist aber auch die Erkenntnis, dass diese Verbote zumindest technisch durchaus umgangen werden können. Die Nutzung von SSL-Verschlüsselung oder auch von Proxy-Servern hebeln die Kontrollmöglichkeiten leicht aus. Wenn aber solche Sperrungen auch in die Dienstvereinbarung zur Internet-Nutzung eines Unternehmens aufgenommen werden, weiß zumindest jeder Mitarbeiter dass ihm Sanktionen bei Zuwiderhandlung drohen.

Auf der anderen Seite gehört aber ein freier Umgang mit den Informationsmöglichkeiten des Internets auch zu einem motivierten und produktiv einsetzbaren Mitarbeiter. Bei zugelassener Nutzung von Social Networks auch vom Arbeitsplatz aus sind die Mitarbeiter aber unbedingt auf die damit verbundenen Gefahren konkret hinzuweisen. Jeder sollte sich darüber im Klaren sein, welche Auswirkungen seine Aktivitäten für ihn selber, das Unternehmen und auch das Unternehmensnetz haben könnten. Es ist auch sinnvoll in gewissen Abständen zu prüfen, welche Informationen über das Unternehmen im Internet eigentlich zur Verfügung stehen. Nicht selten bringt so eine Eigenrecherche brisante Details zutage.

Sollten diese Informationen widerrechtlich nach außen gelangt sein, muss man versuchen, die Verursacher zu ermitteln und sich für die Zukunft auch intensiver mit dem Thema Data Leakage Prevention beschäftigen. Nicht zu vergessen ist natürlich auch der wachsende Anteil von mobilen Geräten mit geschäftlicher Nutzung. Dabei sind zwingend Richtlinien für deren sichere Nutzung zu erlassen und durch geeignete Schutzmaßnahmen (Physischer Schutz, Zugangskontrolle, Malware-Scanner usw.) zu unterstützen.

Detlef Weidenhammer

Literatur:

[1] Bringing Social Security to the Online Community, 2009 http://www.cmocouncil.org

[2] Sophos Security Threat Report 2010 http://www.sophos.com/sophos/docs/eng/papers/sophos-security-threat-report-jan-2010-wpna.pdf

[3] The Privacy Jungle: On the Market for Data Protection in Social Networks", 2009 http://preibusch.de/publications/social_networks/privacy_jungle_dataset.htm

[4] A Practical Attack to De-Anonymize Social Network Users, 2010 http://www.iseclab.org/papers/sonda-TR.pdf

[5] Tips zu Facebook-Profileinstellungen http://www.sophos.de/security/best-practice/facebook-profile.html