

Internet-Sicherheit: Quo vadis?

Dr. Kurt Brand, Pallas GmbH

In Kurzfassung erschienen in: Computer Zeitung, 23.01.2006

Das Internet ist volljährig, jedenfalls wenn man seine Lebenszeit betrachtet. Und die halbe Zeit schon schlagen wir uns mit Viren und Spam herum. Dass die Bedrohung eher noch zunimmt, wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) voraussagt, liegt an der wachsenden Komplexität und der Kommerzialisierung der Internet-Kriminalität. Die Internet-Sicherheit begegnet dem mit integrierten Lösungen (Unified Threat Management) und Managed Services. Und muss weiter auf Bewusstseinsbildung setzen, denn der Mensch ist immer noch die größte Schwachstelle. Letztlich entscheiden die Nasen über die Sicherheit und nicht die Kisten. Und dass der deutsche Mittelständler durchweg 1.500 € jährlich pro Mitarbeiter durch Spam verliert, dieses Bewusstsein von Effizienzverlust durch mangelnde Internet-Sicherheit muss sich auch erst noch durchsetzen.

Spätestens seit Mark Twain wissen wir, dass Prognosen schwierig sind, besonders, wenn sie die Zukunft betreffen. Bei der Internet-Sicherheit ist das Problem noch größer, denn durchgängige Begriffsbestimmung und Bewertung sind schon in der Gegenwart rar. So wird z.B. in einem Firewall-Anbieterprospekt von Sicherheitspaket, Sicherheitslösung und Sicherheitskonzept gesprochen, ohne zu erläutern, was hier wirklich verkauft werden soll. Und so versprach die Finanzbehörde Anfang 2005 "Das Sicherheitskonzept von ELSTER garantiert die sichere Übertragung und Verarbeitung" und suggerierte dem Steuerberater, dass seinem Internet-PC schon nichts passieren könne. Von notwendiger Firewall und Virenschutz war in diesem Zusammenhang keine Rede. Dass ELSTER dann wegen mangelhafter Authentifizierung ins Gerede kam, lenkt vom Hauptproblem eigentlich nur ab.

Was ist Internet-Sicherheit?

Der Begriff Internet-Sicherheit hat viele Facetten und wird auch noch unscharf benutzt. Besonders fatal ist es, wenn Internet-Sicherheit nur punktuell angepackt wird. Da das schwächste Glied die Stärke der Sicherheitskette bestimmt, ist

punktuelle Sicherheit herausgeworfenes Geld. Eigentlich muss dieser eher unfertige Gesamtzustand verwundern, haben doch Internet und Email bereits eine Historie von mehr als zwanzig Jahren. Außerdem sind World Wide Web, Viren und Spam mittlerweile schon zehn Jahre oder länger bekannt.

Internet-Sicherheit ist ein Teil der IT-Sicherheit und adressiert die eher dynamischen Bedrohungen, denen mit operati-

ven Maßnahmen begegnet werden muss. Die weiteren Sicherheits-Bedrohungen können oft schon mit statischen Richtlinien behandelt werden, siehe Abbildung 1.

"Aufpassen und Mitdenken" ist dabei diejenige Sicherheitstätigkeit, der auch künftig die höchste Bedeutung zukommt. Denn der Mensch ist und bleibt die größte Schwachstelle, Sorglosigkeit und Naivität richten mehr Schaden an als kriminelle Innentäter. Wer nicht mitdenkt und nicht misstrauisch wird, wenn ihm unerwartet einige zehntausend Euro aufs Konto kommen, die er nach Abzug einer großzügigen "Aufwandsentschädigung" nur einfach weiterreichen soll, der lässt sich wohl auf Geldwäsche ein. Wer entrüftet und ohne nachzudenken auf die unerwartete eBay-Mahnung klickt, läuft Gefahr, einen Trojaner zu installieren. Und selbst auf die phantastischen Geschichten der "Nigeria Connection" fallen immer noch genug raffigieriger Internet-Nutzer herein.

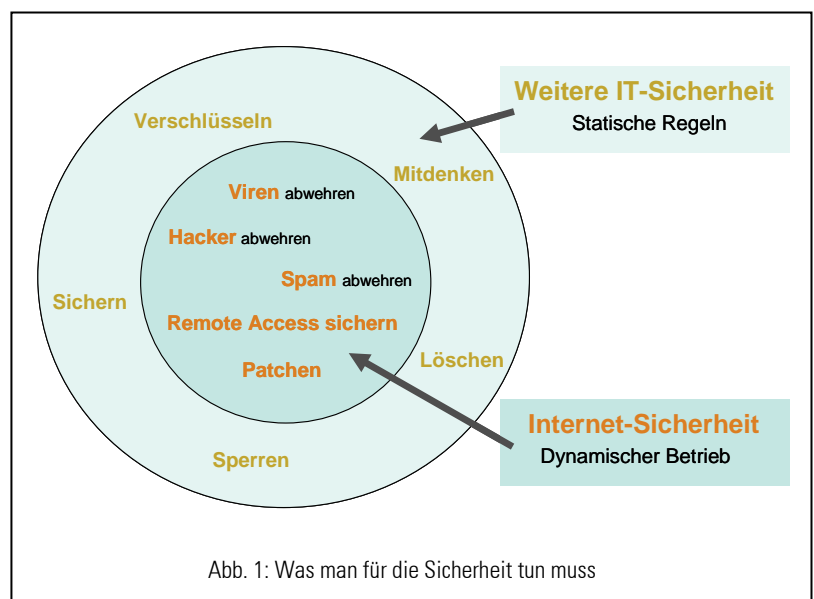


Abb. 1: Was man für die Sicherheit tun muss

Schwache Internet-Sicherheit = niedrige Rendite

Schwache Internet-Sicherheit erzeugt in erster Linie Effizienz- und damit Renditeverluste. Deutsche Mittelständler bearbeiten täglich bereits mehr als eine Stunde lang Emails und verlieren dabei durchweg mehr als 10 Minuten durch Spam. Das klingt erst einmal nicht kritisch, summiert sich aber auf 33 Stunden im Jahr oder etwa 1.500 €Verlust pro Mitarbeiter. Und das ist eine Menge, wenn man bedenkt, dass die Rendite pro Mitarbeiter je nach wirtschaftlicher Lage nur einige tausend Euro beträgt. Diese Tatsache muss der Mittelständler noch besser verinnerlichen. In großen Unternehmen sorgt die Zeiterfassung schon dafür, dass der Renditeverlust auffällt. Immerhin ist erkennbar, dass auch der Mittelstand langsam ein geschärftes Sicherheitsbewusstsein entwickelt. In einer Befragung von Netzwerk elektronischer Geschäftsverkehr und Market Research & Services rangierte das Thema Ende 2004 hinter der Konjunktur bereits an Position 2. Die Empfehlung dieser Studie wie auch vieler anderer Experten heißt: integrierte Sicherheits-Lösungen durch Managed Services einrichten. Das geht sehr gut bei der Internet-Sicherheit, da ein einfacher Wirkungspunkt am Übergang zwischen Unternehmensnetz und Internet vorhanden ist.

Sicher gibt es eine Relation zwischen der Größe einer Firma und ihrer Möglichkeit, Security Services selbst zu erbringen. Ein Unternehmen mit einigen zehn Mitarbeitern kann

normalerweise nur auf externe Services setzen, wohingegen bei einigen hundert Mitarbeitern eine steuernde Kompetenz im eigenen Unternehmen verbleiben kann oder muss. Aber auch die ganz Großen sourcen die Sicherheit aus, häufig als Captive Outsourcing an ihre ehemalige IT-

Abteilung, die jetzt selbständig ist und Kundenservice üben muss. Dabei muss der Mittelstand - anders als die Großen - noch lernen, dass der größte Teil des Aufwands in den Betrieb fließt: Nicht die Kisten entscheiden über die Sicherheit, sondern die Nasen!

Integrierte Managed Security Services

Integrierte Sicherheit ist auch deshalb wichtig, weil die Bedrohungen zusammenwachsen: Würmer schalten die Desktop-Firewall aus, Trojaner installieren Spionageprogramme, und Botnetze versenden Spam oder Denial-of-Service-Angriffe. Weil die Zeiten von Stand-alone-Lösungen vorbei sind, stellt Kerio seine kostenfreie Desktop-Firewall ein. Künftige Angriffe werden smarter, nicht vom internen Ranking der Kiddies getrieben, sondern kommerziell ausgerichtet. Ziele werden nach Schwierigkeitsgrad und Gewinnerwartung ausgewählt, dann schnell und eher still angegriffen. Neue Bedrohungen tun sich durch die Konvergenz von Sprach- und Datendiensten auf. Kürzere Reaktionszeiten in komplexeren Umgebungen sind die notwendige Antwort. Die Abb. 2 zeigt, wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) die künftige Bedeutung verschiedener Gefahrenbereiche sieht.

	Erwartete künftige Bedeutung	Sicherheits-tätigkeiten
1. Irrtum und Nachlässigkeit	↘	Mitdenken
2. Viren, Würmer, Trojaner	↗	Viren abwehren
3. Informationsdiebstahl	↘	Verschlüsseln
4. Software-Fehler	↘	Patchen
5. Hacking	↑	Hacker abwehren
6. Hardware-Fehler	↓	Sichern

Abb. 2: Die Lage der IT-Sicherheit in Deutschland, BSI, Juli 2005

Auch die Abwehrtechnik soll smarter werden, z.B. durch Self Defending Networks, Outbreak/Zero-Hour Virus Protection und Unified Threat Management.

Ohne Zweifel kann mit Security Service Geld verdient werden, und auch in diesem

Bereich mag die Zukunft neue Erfahrungen bringen. Microsoft hat durch den Einsatz von Spam-Fallen und hinreichendem juristischen Druck bereits mehr als 800 Millionen US-\$ von Spammern abkassiert. Davon gingen neulich 250 Tausend US-\$ an einen Schüler, dessen Verdienst es war, den Sasser-Programmierer zu verpfeifen. Hoffentlich wird daraus kein geschlossener Wirtschaftskreislauf.

Wir stellen das Eingangszitat auf den Kopf und sagen mit dem amerikanischen Kybernetiker Hermann Kahn: "Heute kommt es darauf an, aus der Zukunft zu lernen." Die wichtigsten Empfehlungen für diesen Lernprozess zur besseren Internet-Sicherheit sind:

- Sicherheitsrichtlinie verabschieden und befolgen
- Mehrstufige Firewall und stundenfrischen Virens Scanner verwenden
- Spamfilter gegen Effizienzverlust einsetzen
- Ganzheitliche, integrierte Lösungen anstreben
- Managed Security Services nutzen

Internet-Sicherheit einfach mieten

Die Pallas GmbH sorgt für integrierte Internet-Sicherheit zur festen Miete, angepasst an den konkreten Schutzbedarf und ohne Bindung an Investitionen. Pallas betreibt abgesicherte Internet-Server und Applikationen und berät bei der Netzwerksicherheit. Pallas hat den ASP Award gewonnen und wurde durch die Landesinitiative "secure-it.nrw" ausgezeichnet.

Dr. Kurt Brand
Geschäftsführer Pallas GmbH

Weitere Informationen

Dr. Kurt Brand
Pallas GmbH
Hermülheimer Straße 10
50321 Brühl
Tel: 02232-1896-0
Fax: 02232-1896-29
Kurt.Brand (at) pallas.de
www.pallas.de