



Sicherheit als geschäftskritischer Faktor: Wie sich Sicherheit bezahlt macht



Sicherheit als geschäftskritischer Faktor: Wie sich Sicherheit bezahlt macht

Informationen sind der Rohstoff unserer Zeit. Von ihrer Verfügbarkeit und Sicherheit hängt weitgehend der Erfolg moderner Unternehmen ab. Doch die Bedrohungsszenarien für lebenswichtige Informationen und Daten in den Unternehmen werden zunehmend heimtückischer und komplexer. Während wir in der Vergangenheit in erster Linie von Auswirkungen etwa auf die Ausfallzeit von Hardware gesprochen haben, geht es heute um viel mehr:

- ▶ Verlust geistigen Eigentums
- ▶ Identitätsdiebstahl
- ▶ Haftungsansprüche
- ▶ Rufschädigung

Diese negativen Konsequenzen für den Unternehmenserfolg verlangen ein Umdenken über alle Abteilungen hinweg. Heute sind auch die Unternehmensleitung sowie das Operations- und Finance/Legal-Department gefordert.

„IT-Sicherheit kostet nur Geld“: In vielen Unternehmen herrscht noch immer die Denkweise vor, Sicherheit bringe keinen Ertrag und verursache nur Kosten. Dabei sollte IT-Sicherheit Chefsache sein. Sie sollte für Geschäftsführer und Vorstände gleichermaßen gelten und in das Kalkül des operationellen Risikos mit einbezogen werden. Denn gerade Geschäftsführer und CIOs haben für den lückenlosen Schutz der Unternehmensdaten Sorge zu tragen. In einem mangelhaft geschützten Unternehmen riskiert der Geschäftsführer eine persönliche Haftung, die sich auch auf sein persönliches Vermögen erstrecken kann (siehe hierzu das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich, KonTraG). Eine schlechte Security-Leistung kann sich sogar dahingehend auswirken, dass nach Basel II ein schlechteres Unternehmensrating erfolgen kann.

Während Kürzungen an der IT-Sicherheit kurzfristig ein klar sichtbares Sparpotential bieten, führen Schadensberechnungen im Risikomanagement meist nur zu sehr theoretischen Ergebnissen. Einsparungen an der falschen Stelle können jedoch mittelfristig zu teuren Nachinvestitionen führen oder den Verlust von Werten

Schadprogramme im Aufwind			
	2007	2006	Wachstum
TrojWare	201.958	91.911	119,73%
VirWare	12.416	6.282	97,64%
MalWare	5.798	4.558	27,20%
AdWare	14.382	2.583	456,79%
RiskWare	2.690	nicht erfasst	nicht erfasst
Total	237.244	105.334	125,23%

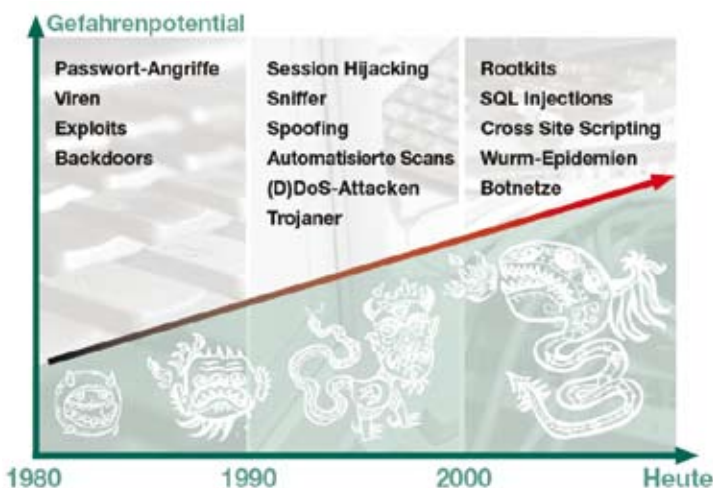
verursachen. Um diese Aufgabe erfüllen zu können, muss der Sicherheitsbeauftragte eines Unternehmens die betriebswirtschaftlichen Gesamtzusammenhänge verstehen.

Unterschätztes Risiko

In den 90er Jahren und auch zu Beginn des neuen Jahrtausends kam es häufig zu Massenangriffen durch Computer-Würmer, und die Medien berichteten ausführlich darüber. In den letzten Jahren sind solche weltweiten Epidemien fast vollständig ausgeblieben: Die Cyber-Kriminellen verwenden neue, komplexe Angriffsformen und konzentrieren sich auf regionale bis lokale Attacken. Die Öffentlichkeit erfährt darüber kaum etwas. Wird ein einzelnes Unternehmen ausspioniert, bleibt dies entweder unentdeckt, oder aber der Angriff wird aus Angst vor Imageschäden nicht publik gemacht.

Daraus resultiert die subjektive Wahrnehmung, dass die Bedrohungen allgemein abnehmen. Die Bereitschaft, in IT-Sicherheit zu investieren, sinkt. Nach einer Umfrage der Gartner Group sind das Sicherheitsverständnis und deren Umsetzung von Rang 2 auf Rang 4 in den Unternehmen gefallen.

In Wirklichkeit nehmen das Gefahrenpotential und damit das Risiko jedoch zu, sie werden nur unterschätzt: Allein 2007 hat Kaspersky Lab über 200.000 neue Schädlinge registriert, so viel wie insgesamt in den 10 Jahren zuvor. Lediglich die sichtbaren Bedrohungen nehmen teilweise ab: So ist der Anteil infizierter Spam-Mails gesunken – allein aus wirtschaftlichem Denken. Spam ist eine nicht zielgerichtete Verbreitungsmethode, die Ausbeute liegt irgendwo im Promille-Bereich. Gezielte Angriffe, die einen höheren wirtschaftlichen Erfolg für die Cyber-Kriminellen versprechen, müssen andere Wege nehmen. Schädlinge werden individuell für einen bestimmten lokalen Angriff angepasst, Rootkits verschleiern deren Anwesenheit im System. Die für einen erfolgreichen Angriff nötigen Komponenten werden professionell entwickelt und kommerziell auf verschiedenen Plattformen im Internet angeboten. Der frühere Vandalismus ist inzwischen also komplett einer kommerziell ausgerichteten, gut organisierten Malware-Industrie gewichen. Wie in einer gut funktionierenden Zulieferindustrie produziert jeder das, was er am besten kann.



Crimeware as a Service: Was kostet was?

Preise für Werkzeuge und Diebesgut in einschlägigen Online-Foren

Zero-Day-Exploit	50 bis 12.000 US\$
Kompromittierter Computer	6 bis 20 US\$
Botnetz	1000 bis 10.000 US\$
Phishing-Website pro Seite	3 bis 5 US\$
Yahoo Mail Cookie Exploit	3 US\$
Yahoo Mail und Hotmail E-Mail Cookies	3 US\$
Verifizierte gültige Kreditkarte (USA)	1 bis 6 US\$
Verifizierte gültige Kreditkarte (UK)	2 bis 12 US\$
Komplette Identität (mit Kontodaten, Kreditkarte, Geburtsdatum, Sozialversicherungsnummer)	14 bis 18 US\$
Liste mit 29.000 Mail-Adressen	5 US\$
Online-Konto mit durchschnittlich 9.900 Dollar Guthaben	300 US\$
Geprüfter Paypal-Account mit Guthaben	50 bis 500 US\$
Ungeprüfter Paypal-Account mit Guthaben	10 bis 50 US\$
Skype-Account	12 US\$
World-of-Warcraft-Account (1 Monat)	10 US\$

Auch das Diebesgut wie ergaunerte Kreditkartennummern oder Zugangsdaten zu Online-Konten werden in vielen Fällen nicht selbst genutzt, sondern wieder im Internet zum Kauf angeboten. Der Handel läuft dort ähnlich ab wie bei einem typischen Aktionshaus: Entweder man bietet seine „Ware“ zum Festpreis an oder lässt verschiedene Interessenten ihr Höchstgebot abgeben. Gut zu sehen: Eine Liste mit 29.000 Mail-Adressen ist mit einem Preis von 5 Dollar relativ wertlos, der Zugriff auf einen kompromittierten Computer hingegen mit 6 bis 20 Dollar schon einiges wert. Ressourcen wie Botnetze werden typischerweise nicht verkauft, sondern für bestimmte Zeit vermietet.

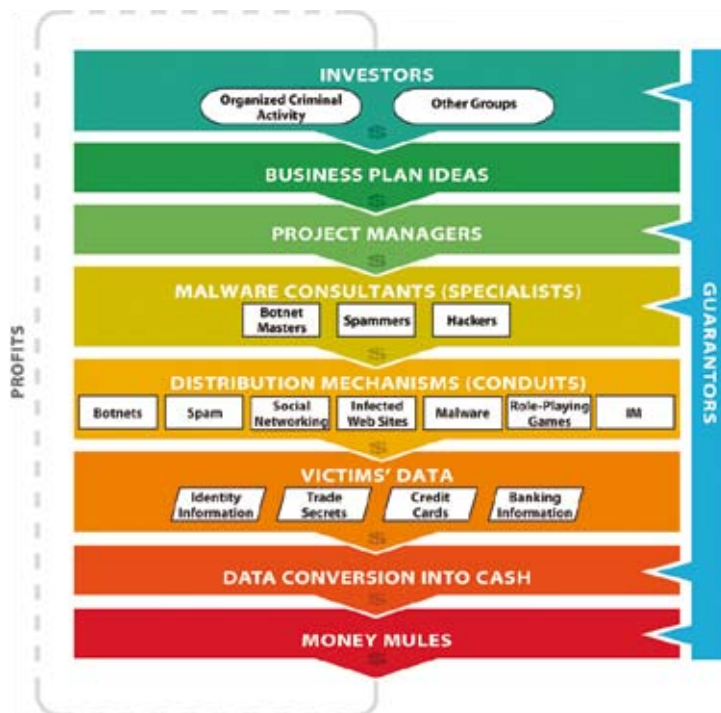
Die Kommerzialisierung der Malware-Szene zeigt sich ganz deutlich im Erscheinungsbild aktueller Schädlinge. Diese arbeiten nicht mehr destruktiv, denn sie sollen ja unerkant bleiben. Außer in Ausnahmefällen – beispielsweise dem Wurm GPCode, der die Daten des Anwenders verschlüsselt um dann von diesem ein Lösegeld zu fordern – richtet Malware keinen Schaden im Dateisystem an. Der infizierte Computer dient ja schließlich als Arbeitsgerät für den Cyber-Kriminellen.

Über 90 Prozent der Computer-Schädlinge sind heute Trojaner – einmal in ein System eingeschleust, verrichten sie dort unbemerkt ihre Arbeit. Drei Viertel der trojanischen Programme richten eine Backdoor ein (über die ein Angreifer Zugriff auf das System erhält), steh-

len Passwörter oder können je nach Bedarf weiteren Schadcode nachladen. Diese Programme verfolgen also ganz klar kommerzielle Ziele, sie sind dazu da, um Informationen zu stehlen.

Infrastrukturen im Wandel

Mit gestiegenen Anforderungen und neuen technischen Möglichkeiten verändert sich auch die Organisation der Firmennetze: Aus den starr strukturierten Firmennetzen sind heute dynamische Netzwerke geworden, in die sich mobile Mitarbeiter von jedem Ort der Welt einklinken können. Sowohl die Gartner Group als auch IDC prognostizieren, dass bis zum Jahr 2013 beziehungsweise 2015 rund 30 Prozent aller Mitarbeiter ständig mobil unterwegs sein werden. Die klassische Perimeter-Sicherheit mit einer Firewall stößt hier an ihre Grenzen: Als reiner Paket-Filter kann diese nur etwa 4 Prozent der täglichen Attacken abfangen. Gegen Spam, Malware und andere Bedrohungen schützt sie nicht. Zudem erfordert die steigende Zahl der Services immer neue Ausnahmen in den Firewall-Regeln: So wird für Anwendungen wie Blackberry ein Loch in die Firewall gebohrt, ebenso für Remote-Access und VPN-Zugänge. Auch Geschäftspartner erhalten manchmal Zugriff auf interne Server, oftmals sogar unverschlüsselt. Sehr deutlich wird das Unvermögen von Perimeter-Firewalls bei Web-Anwendungen, die trotz Firewall anfällig sind für SQL Injections, Web Threat Exploits und anderen bösartigen Code. Auch gegen Fehler in Anwendungs-Software helfen Firewalls nur beschränkt, wie die Würmer CodeRed (Buffer-Overflow durch lange HTTP Get Requests) und SQL Slammer gezeigt haben.



Quantifizierung von Risiken

Die Risiken, denen Unternehmen gegenüber stehen, sind vielfältig. Auch wer sich immer vorsichtig verhält, kann sich heute leicht einen Virus einfangen. Bereits der Besuch einer kompromittierten Webseite reicht aus, um infiziert zu werden. Hacker benutzen immer neue Sicherheitslücken und Applikationsschwächen, um auf die Rechner ihrer Opfer zu gelangen. Durch Verwendung des http-Protokolls werden Paket-Firewalls einfach ausgehebelt, denn HTTP-Verkehr ist meistens erlaubt und kann daher unbehelligt passieren.

Vor Risiken, die im Zusammenhang mit der Übernahme von IT-Systemen und dem Datenabfluss durch Trojaner stehen, schützen Antiviren-Hersteller wie Kaspersky Lab mit vielschichtigen Lösungen. Sie verhindern das Eindringen von Schadsoftware, unterbinden die fremde Kontrolle über Firmenrechner und schützen die dort gespeicherten Informationen, das wichtigste Gut der Unternehmen.

Sicherheit zahlt sich aus

Sicherheit ist ein permanenter Kreislauf, die zu schützenden Assets müssen immer wieder neu bewertet und neu bemessen werden. Doch Sicherheit kostet zunächst einmal Geld und bringt augenscheinlich nicht viel ein. Der Return on Investment (ROI) scheint für viele Unternehmer hier nicht greifbar. In der Tat ist ein konkreter ROI immer schwer nachweisbar.

Der entscheidende Faktor beim Return on Investment als Messgröße über die Ertragskraft eines Unternehmens ist üblicherweise die Amortisationsdauer, also der Pay Off:

$$\text{PayOff in Jahren} = \frac{\text{ursprünglicher Kosteneinsatz}}{\text{Gewinn bzw. Kostenersparnis pro Jahr} + \text{jährliche Abschreibung}}$$

Entscheidend hierbei ist, dass nicht allein der TCO-Gedanke zum Erfolg führt, sondern auch eine Risikobetrachtung den zu erwartenden Verlust minimieren und somit den Gesamtgewinn steigern kann.

Wie eingangs erwähnt, ist IT-Sicherheit heute nicht allein ein Thema für den IT-Verantwortlichen, sondern betrifft alle Abteilungen. So darf etwa die Finanzabteilung bei der Risikobetrachtung nicht einfach die billigste Schutzlösung auswählen, sondern muss auch das verbleibende Risiko berücksichtigen. Im Schadensfall – oder wenn dadurch Nachinvestitionen in zusätzliche Schutzkomponenten nötig werden – kann sich die Billiglösung als sehr teuer erweisen. Auch müssen stets die Kosten für die Implementierung, Schulung etc. mit berücksichtigt werden.

Effektives Risikomanagement

Bereits bei dem Begriff „Risiko“ werden die unterschiedlichen Denkweisen von der Geschäftsführung einerseits und dem Verantwortlichen für Sicherheit andererseits deutlich. Risiko bedeutet für die Führungsebene vor allem eine Gefahr für den vertrieblichen Erfolg – also entgangene Einnahmen oder der Verlust von Reputation. Der Sicherheitsbeauftragte definiert diese Begriffe vollkommen anders – technokratisch – und bezeichnet ein Risiko immer als eine Gefahr für die IT, beispielsweise die Störung oder Übernahme der IT-Systeme durch Hacker. Die Herausforderung für moderne Unternehmen wird also in Zukunft darin bestehen, beide Abteilungswelten mittels einer gemeinsamen Sprache anzunähern.

„Informationssicherheit ist kein Selbstzweck, sondern dient der Absicherung von kritischen Geschäftsprozessen gegen bestehende und zukünftige Gefährdungen“

Eine gängige Argumentation in Unternehmen geht dahin, dass Sicherheit keinen direkt messbaren Ertrag im Unternehmen bringen würde. Oberflächlich betrachtet stimmt das wohl, aber auf den zweiten Blick eben nicht. Denn Verlust – egal, ob er aufgrund mangelnder Vertriebsleistung oder eben aufgrund mangelnder Sicherheitsstrukturen auftritt – reduziert den erwarteten Gewinn merklich. Diese Botschaft muss von den Sicherheitsverantwortlichen in die Führungsebene und damit in das Unternehmen transportiert werden. Sicherheit muss als Förderer der Chancen und damit des Unternehmensgewinns verstanden werden.

Sicherheit lässt sich auch nicht auf Jahre hinaus planen: Ein Geschäftsmodell kann sich ändern, und auch das Bedrohungsszenario unterliegt einem ständigen Wandel. Prozesse müssen aus betriebswirtschaftlicher Sicht immer an diesen Umstand angepasst werden.

Risiken kann man mit unterschiedlichen Strategien begegnen: Akzeptable Risiken kann ein Unternehmen entweder selbst tragen oder beispielsweise über Versicherungen oder Vertragsklauseln abwälzen. Alle sonstigen identifizierbaren Risiken sollten abgewehrt oder wenigstens so weit vermindert werden, wie dies technisch möglich und zugleich wirtschaftlich sinnvoll ist. Typische Fragen, die man sich dabei stellen sollte, sind:

- ▶ Wie teuer wird es, wenn ich gar nichts unternehme?
- ▶ Kann ich mich gegen den Schaden versichern?
- ▶ Was muss ich investieren, um möglichen Schaden abzuwenden? Oder – unternehmerisch – gefragt: Was muss ich tun, um den Geschäftsprozess zu unterstützen, damit kein Verlust des erwarteten Gewinns eintritt?
- ▶ Wie schütze ich mein Unternehmen gegen Reputationsverlust?

KONTAKT



● **Kaspersky Lab Central Europe**
 Steinheilstraße 13
 85053 Ingolstadt
 Deutschland
www.kaspersky.de
 Email: info@kaspersky.de
 Tel. +49 (0) 841 98 18 90

● **Kaspersky Lab HQ**
 Russland, Moskau 123060
 Pervij Wolokolamski Proyezd
 d. 10, str. 1
 Russia
www.kaspersky.ru
 Email: sales@kaspersky.com
 Tel. +7 495 797 8700

● **Kaspersky Lab USA**
 500 Unicorn Park
 Woburn MA 01801 USA
www.kaspersky.com
 Email: info@us.kaspersky.com
 Tel. +1 781 503 1800

● **Kaspersky Lab UK**
 E1 Atrium
 Culham Science Centre
 Abingdon, Oxon, OX14 3DB
 United Kingdom
www.kaspersky.co.uk
 Email: info@kasperskylab.co.uk
 Tel. +44 (0) 1865 408566

● **Kaspersky Lab France**
 92500 Rueil Malmaison
 ZAC. Rueil 2000
 2, rue Joseph Monier
 Immeuble l'Europeen, Batiment C
 France
www.kaspersky.fr
 Email: info@fr.kaspersky.com
 Tel. +33 1 41 39 04 44

● **Kaspersky Lab Benelux**
 Hambakenwetering 10
 5231 DC 's-Hertogenbosch
 The Netherlands
www.kaspersky.nl
 Email: sales@kaspersky.nl
 Tel. +31 (0) 73 615 4860

● **Kaspersky Lab Poland**
 Ul. Krotka 27A 42-200
 Czestochowa Poland
www.kaspersky.pl
 Email: info@kaspersky.pl
 Tel. +48 34 368 18 14

● **Kaspersky Lab China**
 Suite A503-507, U-Space Mall, No.8
 Guang Qu Men Wai Street
 Chaoyang District, Beijing 100022
 China
www.kaspersky.cn
 Email: sales@kaspersky.com.cn
 Tel. +86 10 58612570

● **Kaspersky Lab Japan**
 Higashi Kanda Towa, 6F 2-3-3
 Higashi Kanda, Chiyoda-ku
 Tokyo, 101-0031
 Japan
www.kaspersky.co.jp
 Email: sales@kaspersky.co.jp
 Tel. +81 3 5687 7830

● **Kaspersky Lab Korea**
 Floor 7 Sindo Building 1604-22
 Seocho-dong, Seocho-gu, Seul
 Korea
www.kasperskylab.co.kr
 Email: sales@kasperskylab.co.kr
 Tel. +82 2 508 8789



Kaspersky Labs GmbH
Steinheilstr. 13 • 85053 Ingolstadt • Deutschland

E-Mail: info@kaspersky.de
Telefon +49 (0) 841 98 18 90
www.kaspersky.de

Kaspersky Security ist das eingetragene Warenzeichen von Kaspersky Lab.
Alle anderen Namen sind die Warenzeichen ihrer Eigentümer.

© 2008 Kaspersky Lab, Ltd