

IT-security

Studienband 2003

0. Kommentar
1. Sicherheitsbewusstsein
2. Sicherheitsmaßnahmen
3. Sicherheitsrichtlinien
4. Sicherheitsverletzungen
5. Budgets und Verantwortlichkeiten
6. Statistik
7. Erhebungsdesign

Kommentar

Trotz der steigenden Zahl und Komplexität der Sicherheitsbedrohungen wiegen sich deutsche wie amerikanische Unternehmen gleichermaßen in der Sicherheit, ausreichend Vorsorge getroffen zu haben. Die vorliegende InformationWeek-Studie IT-Security 2003 gibt Aufschluss darüber, wie die Sicherheitslage in deutschen Unternehmen tatsächlich ist. Bei der nunmehr sechsten Studie haben wir die Situation in Deutschland mit der in den USA gegenüber gestellt. Ergebnis-Aufbrüche haben wir für die drei Branchen Behörden, produzierende Industrie sowie Dienstleistungsbranche beigefügt. Die genaue Zusammensetzung der Stichprobe finden Sie im Kapitel »Statistik«.

Heiße Tage, schlaflose Nächte – das war der Sommer 2003

Unmittelbar nachdem die Befragung zur diesjährigen IT-Security-Studie im Feld war, brach in deutschen Unternehmen ein Chaos los: Systemadministratoren hatten bei der Jahrhunderthitze nicht nur alle Hände voll zu tun, ihre Serverräume zu kühlen. Seit dem elften August hielt sie zudem eine Serie von Viren und Würmern auf Trab.

Der Wurm Lovesan, auch als MSBlast oder Blaster bekannt, hat innerhalb von nur 24 Stunden mehrere hunderttausend Rechner weltweit infiziert. Betroffen waren vor allem Anwender von Windows NT, 2000, XP und 2003.

Im Gegensatz zu Würmern, die sich per E-Mail verbreiten, agiert Lovesan ohne Zutun des PC-Nutzers. Mittlerweile sind schon Varianten von MSBlast im Umlauf, die Backdoor-Trojaner installieren. Damit werden infizierte Rechner für unautorisierte Anwender sowohl zugänglich als auch kontrollierbar.

Microsoft hatte Mitte Juli vor der Gefahr eines Buffer Overflows an Port 135 gewarnt und einen Patch bereitgestellt. Noch einfacher hätten sich Anwender durch Sperrung des Ports 135 ihrer Firewall behelfen können.

Anwender hatten noch nicht einmal die Folgen von Lovesan im Griff, da überrollte Sobig.f die Rechner aller Kontinente. Dieser Wurm schleicht sich nicht über Schwachstellen ein. Der Anwender muss die im

Anhang einer E-Mail verschickte Datei selbst öffnen, damit Sobig.f in den Computer eindringen kann. Um eine Verbreitung des Wurms zu garantieren, hat sein Autor Spam-Technologien zum Massenversand verwendet. »Sobig.f kann nur mit der immer noch wütenden Lovesan-Epidemie verglichen werden,« so Denis Zenkin, Pressesprecher des russischen Antiviren-Unternehmens Kaspersky Labs. »Doch während Lovesan in erster Linie für das Internet eine Bedrohung darstellt, weil es dieses verlangsamt, ist Sobig.f eine reale Gefahr für die User. Mit diesem Wurm kann dessen Autor volle Kontrolle über die infizierten Computer gewinnen.«

Virenvorfälle dominieren

Dass die Virenproblematik auch in den Firmen nach wie vor höchste Brisanz besitzt, zeigen die Ergebnisse der aktuellen InformationWeek-Studie zur Informationssicherheit in Unternehmen. Danach war fast die Hälfte der befragten deutschen Unternehmen jeder Größe und Branche von Computerviren, Trojanern und Würmern betroffen.

Auch in den USA richtete Malicious Code bei 46 Prozent der Firmen Schäden an. Dabei stieg die Zahl der durch Sicherheitsverstöße bedingten finanziellen Verluste amerikanischer Unternehmen im Vergleich zum Vorjahr deutlich an. So gab gegenüber 2002 die dreifache Anzahl an Befragten (sechs Prozent) an, Verluste über 500.000 Dollar erlitten zu haben.

Besonders alarmierend: Rund ein Sechstel der amerikanischen wie deutschen Befragten weiß überhaupt nicht um mögliche Sicherheitsbedrohungen. Die Gründe dafür sind vielfältig und Dauerbrenner in den Unternehmen.

Laut Ergebnissen der Studie macht 60 Prozent der befragten deutschen Firmen die zunehmende Zahl und Komplexität der Sicherheitsbedrohungen zu schaffen. So ermittelte das CERT Coordination Center, eine Institution der Carnegie-Mellon-Universität, 76.404 Sicherheitsverstöße innerhalb der ersten sechs Monate dieses Jahres, verglichen mit 82.094 für das gesamte Jahr 2002. Und Hersteller von Antivirenlösungen verzeichnen zunehmend Bedrohungen, deren Komplexität steigt. So betrug der Anteil der so genannten Blended Threats, die der Sicherheitsanbieter Symantec in der zweiten Hälfte des Jahres 2002 analysierte, 80 Prozent.

Angesichts der steigenden Anforderungen steht in den meisten Unternehmen viel zu wenig Personal zur Verfügung. Ein Fünftel der befragten deutschen Firmen klagt – wie im vergangenen Jahr – über mangelnde Besetzung von IT-Security-Positionen. In den USA sind es in diesem Jahr sogar 31 Prozent, denen es an Personal fehlt. Dass die Sicherheitsverantwortlichen über zu wenig Zeit für ihre Aufgaben klagen, wundert daher nicht.

Ein Lichtblick: Waren es im vergangenen Jahr noch 72 Prozent, die unter der Arbeitslast ächzten, ging die Zahl in diesem Jahr auf 57 Prozent zurück. Konstant geblieben ist die Zahl derer, denen die Hände infolge knappen Budgets gebunden sind. So gaben – wie im vergangenen Jahr – 54 Prozent der befragten deutschen Unternehmen an, der Sparzwang gefährde dringend notwendige IT-Security-Projekte – gegenüber 45 Prozent aus den USA. Es scheint sich nach mehreren aufeinander folgenden Jahren steigender Sicherheitsinvestitionen ein gefährlicher Trend abzuzeichnen: In der Befragung gaben 57 Prozent der deutschen IT-Manager an, in diesem Jahr nicht mehr als im Vorjahr ausgeben zu können. In den USA sind es nur 42 Prozent, die mit einem IT-Security-Budget in der Höhe von 2002 auskommen müssen. Und 39 Prozent der amerikanischen Unternehmen haben in diesem Jahr mehr in IT-Security investiert als noch im letzten Jahr. Deutschland kommt nicht einmal auf ein Viertel.

Budget und Verantwortlichkeiten

Verantwortlichkeiten für die Umsetzung von Security sowie die Definition der Sicherheitsrichtlinien und die Budgetverantwortlichkeit driften auseinander. Zwar ist es die IT, die in den meisten Fällen für Security und entsprechende Maßnahmen den Kopf hinhalten muss, aber kaufmännische Entscheider haben immer öfter das Sagen, wenn es um Budgethöhen beziehungsweise die Verwendung der Mittel geht.

Etwas über die Hälfte der befragten Unternehmen geben an, das IT-Security-Budget sei Teil des IT-Budgets. Dabei macht der für Security reservierte Teil knapp zwölf Prozent des IT-Budgets aus und liegt damit anteilig etwas höher als beispielsweise in den USA. Allerdings ist der Durchschnittswert stark von Unternehmensgrößen abhängig. So geben Großunternehmen mit mehr als 5.000 Mitarbeitern lediglich 7,2 Prozent ihres IT-Budgets für Security aus.

Knappe Budgets sind eines der Haupthindernisse für die Sicherheit der Unternehmens-IT. Rund 55 Prozent der

befragten Unternehmen klagen direkt über zu geringe Budgets. Ein eben so großer Teil klagt über Zeitmangel, was indirekt auf Ressourcenknappheit schließen lässt und ebenfalls dem Problemkreis Budget zuzurechnen ist. Über Budgetmangel klagen vor allem mittelständische Unternehmen mit 101 bis 500 Mitarbeitern.

Ein Blick auf die Budgets gibt schnellen Aufschluss über die Ursache dieser Klagen: Jedes dritte Unternehmen gibt an, für IT-Security ein Budget bis 10.000 Dollar reserviert zu haben. Untersucht man genauer, wie weit diese Summe trägt, stellt man schnell fest, dass es mit der Sicherheit nicht allzu gut bestellt sein kann. Denn eine kleine Firewall-Appliance allein schlägt mit rund 2.500 Euro zu Buche und muss anschließend noch installiert, konfiguriert und fortlaufend betreut werden. Bereits diese Anschaffung verschlingt damit über die Hälfte des Security-Budgets vieler befragter Unternehmen.

Das Spiel mit der Angst

Ein wesentlicher Schwachpunkt im Poker um höhere IT-Security-Budgets ist die Argumentation der Verantwortlichen. In den meisten Fällen ist es das Spiel mit der Angst: Risikobegrenzung (70 Prozent Nennungen) sowie potentielle Haftung beziehungsweise mögliche Risiken (52 Prozent) werden hier genannt. Auswirkungen auf das Geschäftsergebnis spielen nur für rund 29 Prozent der Befragten eine Rolle. Die Gesetzeslage wird lediglich von knapp 40 Prozent ins Feld geführt.

Signifikant ist der Unterschied zu den USA. Allgemeine Risikobegrenzung nennt nur jedes vierte Unternehmen als Faktor. Wichtiger sind Haftung beziehungsweise mögliche Risiken mit zwei Dritteln der Nennungen. Über die Hälfte bringt gesetzliche Anforderungen ins Spiel. Kaufmännische Überlegungen spielen immerhin noch für rund 40 Prozent der Befragten eine wichtige Rolle.

Da wie gesehen allerdings kaufmännische Verantwortliche immer häufiger über Budgethöhen bestimmen, erscheint gerade eine kaufmännische Argumentation als eines der Kriterien mit der höchsten Erfolgsaussicht.

Wo genau das Problem der Verantwortlichen mit kaufmännischen Überlegungen liegt, zeigt sich, wenn man Auswirkungen von Sicherheitsvorfällen betrachtet. Ausfallzeiten etwa sind bei vielen Unternehmen nur schlecht erfassbar. Sehr problematisch wird es, sollen die Verantwortlichen nachgewiesene Ausfallzeiten in Geld quantifizieren: Während 32 Prozent der Befragten angeben, keine Ausfallzeiten durch Sicherheitsverstöße erlitten zu haben, konstatieren 42 Prozent keinen finanziellen Schaden. Allerdings implizieren Ausfälle bei wichtigen Systemen immer auch monetäre Auswirkungen, wenn auch nur indirekte. Das lässt den Schluss zu, dass innerhalb der IT im Allgemeinen und bezüglich IT-Security im Speziellen nur unzureichende Kostentransparenz in den Unternehmen herrscht. So ist es auch nicht verwunderlich, dass die wenigsten Verantwortlichen

kaufmännische Argumentationen für die Realisierung von Sicherheitsmaßnahmen anführen.

Hier ist es unbedingt nötig, dass die Verantwortlichen umdenken. Dass es diese Tendenz gibt sieht man bei Großunternehmen mit mehr als 5.000 Mitarbeitern. Hier spielt die Finanzierung von IT-Sicherheit bereits heute eine sehr zentrale Rolle.

Mangelndes Problembewusstsein und fehlende Konsequenz

Mangelndes Problembewusstsein und fehlende Konsequenz in der Umsetzung der Sicherheitsrichtlinien sind heute eines der größten Probleme der IT-Security. Vor allem bei größeren Organisationen werden mangelndes Problembewusstsein und fehlende Kooperation zwischen den einzelnen Abteilungen als Hauptbarrieren für die Effizienz von Sicherheitsmaßnahmen genannt. Wenig überraschend steht »Schaffung eines Sicherheitsbewusstseins« bei rund 40 Prozent der befragten Unternehmen ganz oben auf der kurzfristigen Agenda.

Beinahe ein Drittel der konstatierten Sicherheitsverstöße geht auf das Konto von nicht autorisierten Mitarbeitern. An erster Stelle rangieren Hacker, was mit der Häufigkeit von Virenvorfällen korrespondiert. Interessant ist die Betrachtung nach Unternehmensgrößen: Während bei mittleren und kleinen Unternehmen der Faktor Fehlverhalten der Mitarbeiter eine kleinere Rolle spielt, nimmt dessen Bedeutung bei Großunternehmen dramatisch zu. Fast drei Viertel der Unternehmen mit mehr als 5.000 Beschäftigten macht heute eigene Mitarbeiter für Sicherheitsverstöße verantwortlich. Angesichts des deutlichen Gefälles ist davon auszugehen, dass viele mittelständische und kleine Unternehmen tatsächlich nicht in der Lage sind, Angriffe von innen zu identifizieren.

Nach der Risikotoleranz hinsichtlich Sicherheitsrichtlinien und –maßnahmen befragt, charakterisiert sich die überwältigende Mehrheit der befragten Unternehmen (67,3 Prozent) als moderat, knapp neun Prozent sogar als abgeneigt.

Moderat bedeutet in Konsequenz, dass die Einhaltung der Richtlinien und die Nutzung der installierten Maßnahmen nur unzureichend überwacht beziehungsweise von den Verantwortlichen durchgesetzt werden. Gefragt sind hier vor allem Nicht-IT-Verantwortliche wie die Unternehmensleitung und die Leiter der einzelnen Fachabteilungen.

Allerdings ist bei lediglich einem Fünftel der befragten Unternehmen IT-Sicherheit Chefsache, bei den meisten ist die Verantwortung innerhalb der IT angesiedelt. Die Fachabteilungen werden in Sicherheitskonzepten kaum einbezogen beziehungsweise für deren Umsetzung auf Mitarbeiterlevel verantwortlich gemacht.

Ein hinreichender Schutz der Unternehmens-IT vor Übergriffen lässt sich nur garantieren, wenn das Sicherheitsbewusstsein von der Geschäftsleitung in die gesamte Organisation getragen und die Umsetzung entsprechend kontrolliert wird. Grundlegend falsch ist es, Bedrohungen von aussen mit immer ausgefeilteren technischen Mitteln zu begegnen, aber die

einfachsten internen Maßnahmen zu vernachlässigen. Noch immer sind Passworte unter der Tastatur beziehungsweise auf Post-Its am Monitor in vielen Unternehmen die Regel. Der Einsatz von Memory-Sticks und die Verbreitung von Notebooks machen es heute schwierig, die Sicherheit kritischer Unternehmensdaten zu kontrollieren.

Erst wenn das Gros der Mitarbeiter Sicherheitsmaßnahmen nicht mehr als Gängelung oder Komplizierung der eigenen Arbeitsabläufe begreift, kann umfassender Schutz gewährleistet werden. Ansonsten wird die Tendenz, Work-Arounds zu schaffen und Sicherheitseinrichtungen zu umgehen, Eindringlingen Tür und Tor öffnen.