Mit bester Empfehlung von TREND MICRO

IT-Sicherheit

FÜR

DUMMIES®

Trend Micro Ausgabe für kleine Unternehmen

Schützen Sie Ihr Unternehmen

GRATIS eTips auf dummies.com®

IT-Sicherheit

FÜR

DUMMIES®

KLEINE UNTERNEHMEN

von Trend Micro

WILEY

A John Wiley and Sons, Ltd, Publication

Kleine Unternehmen: IT-Sicherheit Für Dummies®

Veröffentlicht von
John Wiley & Sons, Ltd
The Atrium
Southern Gate
Chichester
West Sussex
PO19 8SQ
England

Weitere Informationen zur Erstellung eines individuellen *„Für Dummies"*-Buches für Ihr Unternehmen oder Ihre Organisation erhalten Sie von CorporateDevelopment@wiley.com. Weitere Informationen zur Lizenzvergabe der Marke *„Für Dummies"* für Produkte und Dienstleistungen erhalten Sie von BrandedRights&Licenses@Wiley.com.

Besuchen Sie uns im Internet unter www.customdummies.com

Wiley veröffentlicht Bücher auch in verschiedenen elektronischen Formaten. Es kann daher sein, dass einige Inhalte zwar in gedruckter, nicht aber in elektronischer Version zur Verfügung stehen.

ISBN: 978-0-470-66692-0

Gedruckt und gebunden in Großbritannien von Page Bros, Norwich

10 9 8 7 6 5 4 3 2 1

Einleitung

Sie kennen die Auswirkungen, die Viren, Spam und Spyware auf Computer haben: infizierte Dateien, blockierte E-Mail-Systeme und plötzlicher Ausfall von Geräten, die eigentlich voll funktionstüchtig sind. Was bedeutet das für Ihr Unternehmen? Sind die grundlegenden Sicherheitsmaßnahmen, die Sie bislang ergriffen haben, wirklich ausreichend? Würden Sie bemerken, wenn sich in Ihrem Netzwerk eine Bedrohung ausbreitet?

Mit weniger Mitteln mehr erreichen – das ist das Gebot der Stunde in vielen Unternehmen, die mit begrenzten Budgets auskommen müssen. Dabei kann es sein, dass die IT-Sicherheit auf der Prioritätenliste einige Stufen nach unten rutscht. Es gibt so viele andere Dinge, auf die man sich konzentrieren muss. Da Ihre IT-Infrastruktur aber von allen Seiten bedroht ist, werden Investitionen in ihre Sicherheit zu immer notwendigeren Betriebskosten.

Man kann es nicht oft genug sagen: Kleine Unternehmen sind besonders anfällig für IT-Bedrohungen, weil sie in der Regel nicht über festangestellte IT-Mitarbeiter verfügen, die sich um alles kümmern. Aber das ist kein Grund zur Sorge: Ihr Unternehmen umfassend zu schützen, ist wahrscheinlich einfacher, als Sie denken. Mit der Lektüre dieses Buches machen Sie den ersten Schritt in die richtige Richtung.

Die Zeit und Mühe, die Sie heute in den Schutz Ihres Unternehmens investieren, gewährleisten langfristige Vorteile: Hohe finanzielle Kosten und Schäden werden vermieden und Ihr Unternehmen kann sich zukünftige Erfolge sichern. Dieses Buch gibt Inhabern kleiner Unternehmen einen Überblick über die Grundlagen der Sicherheit. Dazu gehört eine Darstellung der heutigen und zukünftigen Quellen gravierender Bedrohungen sowie die Analyse einiger neuer Lösungen für die wachsenden Herausforderungen des Sicherheitsmanagements.

Die Mindestanforderung für einen Unternehmensinhaber: Er muss die Bedrohungen und deren mögliche Folgen für sein Unternehmen kennen. Auch die einschlägigen rechtlichen Bestimmungen zu Datenschutz und IT-Sicherheit müssen

bekannt sein und befolgt werden. Zusätzliche Sicherheit wird erzielt durch die Verfassung einer unternehmensweiten Sicherheitsrichtlinie und die Formulierung allgemeiner Internet- und E-Mail-Nutzungsbedingungen für die Mitarbeiter.

Über dieses Buch

Dieses Buch zeigt, dass eine Investition in Sicherheit nicht unbedingt teuer oder zeitaufwändig sein muss. Vielleicht haben Sie ja auch schon viele der notwendigen Sicherheitsmaßnahmen ergriffen und müssen nur noch sicherstellen, dass die verschiedenen Werkzeuge und Schutzvorkehrungen auch zusammenarbeiten.

Sicherheitsinvestitionen sind nicht zwangsläufig umständlich und teuer. Tatsächlich werden Sicherheitslösungen im Gegenteil sogar einfacher und günstiger. Fast täglich berichten die Medien über die Aktivitäten von Cyberkriminellen. Immer öfter werden dabei nicht nur große sondern auch kleine Unternehmen zur Zielscheibe. Der Grund: Die Abwehrsysteme kleinerer Unternehmen sind in vielen Fällen leichter zu überwinden, denn es fehlen die Mittel, die Systeme mithilfe hochqualifizierter Berater hundertprozentig sicher zu machen. Trotzdem sind natürlich auch kleine und mittlere Unternehmen auf die Verfügbarkeit technischer Ressourcen wie Webserver oder Verteilerlisten angewiesen.

Die gute Nachricht ist, dass die Überwachung und Verwaltung von Sicherheitslösungen immer einfacher und günstiger wird. Außerdem werden die integrierten technischen Kontrollen der Anbieter immer ausgereifter und kompakter. Die verschiedenen Möglichkeiten, die entwickelt werden, machen Sicherheit für Unternehmen jeder Größe erschwinglicher.

Die in diesem Buch verwendeten Konventionen

Die *„Für Dummies"* Bücher verfügen über ihre eigenen, bewährten Methoden. Zum Beispiel kann es sein, dass es beim Druck dieses Buches nötig war, einige Internetadressen (die zur besseren Unterscheidung in einer anderen Schriftart erscheinen) über zwei Textzeilen aufzuteilen. Falls dies

vorkommt, können Sie sicher sein, dass wir keine weiteren Buchstaben (wie zum Beispiel Bindestriche) hinzugefügt haben, um die Trennung deutlich zu machen. Wenn Sie also eine dieser Internetadressen verwenden, tippen Sie einfach genau das ab, was Sie im Buch sehen, und ignorieren Sie den Zeilenumbruch.

„Dummies" verwendet ferner Randsymbole, um bestimmte Informationen hervorzuheben. Die Symbole in diesem Buch sind:

Die Information neben diesem Zeichen können Sie sofort in die Praxis umsetzen.

Dieses Symbol weist auf Informationen hin, die Sie im Hinterkopf behalten sollten, während Sie das Thema vertiefen.

Besonders gefährliche Handlungsvorgänge erkennen Sie immer an diesem einschüchternd aussehenden Symbol.

Wie ist dieses Buch aufgebaut?

Die Bereiche, die kleine Unternehmen beim Beheben von IT-Sicherheitsproblemen berücksichtigen müssen, sind in den sechs Kapiteln dieses kleinen Buches abgedeckt. Wir hoffen, dass Ihnen die einzelnen Teilüberschriften Auskunft darüber geben, was Sie über den Inhalt wissen müssen:

- Kapitel 1: Sicherheitsbedrohungen bewerten
- Kapitel 2: Am Anfang steht die Sicherheitsrichtlinie
- Kapitel 3: Ein koordiniertes Abwehrsystem aufbauen
- Kapitel 4: Kenne deinen Feind
- Kapitel 5: Praktische Lösungen ausarbeiten
- Kapitel 6: Die 10 besten IT-Sicherheitsmaßnahmen für kleine Unternehmen

Keine Angst also – bei diesem Buch handelt es sich nicht um ein technisches Handbuch (damit können sich andere Quellen beschäftigen und Ihre technisch versierten Mitarbeiter können sich um die Umsetzung kümmern). Lesen Sie einfach los und erfahren Sie, wie Sie die Sicherheit Ihres kleinen Unternehmens verbessern können!

Kapitel 1

Sicherheitsbedrohungen bewerten

In diesem Kapitel

- Erfahren Sie, was die IT kleiner Unternehmen bedroht
- Beurteilen Sie die mögliche Auswirkungen auf Ihr Unternehmen
- Beginnen Sie, Ihre dringlichsten Probleme nach Priorität zu ordnen
- Erfahren Sie, an welche Regelungen Sie sich halten müssen
- Bewerten Sie die sich verändernde Reaktion der Sicherheitsbranche

In diesem Kapitel werden die Wiederholungstäter identifiziert: also die Sicherheitsbedrohungen, die den Unternehmen immer wieder Probleme bereiten. Außerdem beschäftigt es sich mit den möglichen Auswirkungen dieser Bedrohungen auf Ihr Unternehmen – vom Netzwerkausfall über finanzielle Verluste bis hin zur Tatsache, dass Ihr guter Ruf bei Geschäftspartnern und Kunden geschädigt wird.

Ohne jetzt den unmittelbar bevorstehenden Zusammenbruch der Informationstechnologie auszumalen – es gibt bestimmte Bedrohungen, die Sie kennen müssen, und Regelungen, an die Sie sich halten sollten. Wenn man bei der Planung immer im Auge behält, dass es zu Katastrophen kommen kann, ist man auf ein derartiges Ereignis vorbereitet und behält die Nerven.

Die gravierendsten Bedrohungen erkennen

Seit der Einführung von Computersystemen und Netzwerken in kleinen Unternehmen in den 1980er Jahren wurde die

Sicherheit dieser Systeme immer wieder durch verschiedene Bedrohungen angegriffen. Dabei ist es egal, ob Sie glauben, dass die Gefahrenlage über- oder unterbewertet wird – sicher ist, dass die Bedrohungen nicht einfach verschwinden werden.

Eine halbjährlich durchgeführte Studie zur IT-Sicherheit fand heraus, dass kleine Unternehmen im Durchschnitt von sechs Zwischenfällen pro Jahr berichten – und einige sogar von wesentlich mehr. Sechs Zwischenfälle mag nicht sehr viel sein, aber wenn Sie weniger als 50 Mitarbeiter und keine festangestellten IT-Mitarbeiter haben, ist jede Sicherheitslücke nicht nur ein großes Problem, sie kann auch eine große Belastung für Ihre Ressourcen sein.

Ein Bewusstsein für die Bedrohungen zu entwickeln, ist der erste Schritt, um sich mit ihnen auseinander zu setzen. In Zeiten von Identitätsdiebstahl, Spam und *Spyware* (unerwünschte Software, die heimlich die Benutzeraktivität überwacht, um persönliche Daten zu sammeln und diese weiterzuleiten) werden Sie vielleicht überrascht sein, wie elementar einige der gravierendsten Bedrohungen sein können.

Im Folgenden finden sich die Arten von Zwischenfällen, die in den untersuchten Unternehmen die größten Schäden angerichtet haben, wobei die Ereignisse nach ihrer Häufigkeit gelistet sind:

- Systemausfall oder beschädigte Daten
- Vireninfektion oder störende Software
- Missbrauch der Informationssysteme durch Mitarbeiter
- Unbefugter Zugriff von Außenstehenden (einschließlich Hacker-Angriffe)
- Diebstahl von Computern und Speichermedien
- Diebstahl oder Betrug mithilfe von Computern
- Diebstahl oder unbefugte Weitergabe vertraulicher Daten.

Auch wenn Sie der Meinung sind, dass Ihr Unternehmen bereits vor all diesen Bedrohungen geschützt ist, sollten Sie es sich jetzt noch nicht gemütlich machen: An dieser Stelle müssen wir auf die ständige Veränderung der IT-Berohungen hinweisen.

Vor einigen Jahren stellte zum Beispiel eine Vireninfektion die größte Bedrohung dar: Sie war für die Hälfte aller Sicherheitsvorfälle in der durchgeführten Studie verantwortlich. Heute liegt die Zahl der durch eine Vireninfektion bedingten Vorfälle nur noch bei 21 Prozent, während ein Systemausfall und beschädigte Daten die größere Bedrohung darstellen. Wer weiß also schon, was in ein paar Jahren – oder ein paar Monaten – die Bedrohung Nummer 1 sein wird? In Kapitel 5 geben wir Ihnen darum Ratschläge, wie Sie Ihr System so flexibel halten können, dass es mit allen Problemen der Zukunft zurechtkommt.

Vergessen Sie aber trotz immer ausgereifterer IT nicht, die elementarsten Bedrohungen stets mit in Betracht zu ziehen. Der Missbrauch der Systeme durch Mitarbeiter steht ganz oben auf der Liste der derzeitigen Bedrohungen. Vielleicht wird in einigen Unternehmen vergessen, Fenster und Türen zu schließen, weil Sie zu sehr auf die ausgefeilten Sicherheitssysteme vertrauen.

Glossar der wichtigsten Bedrohungen

Den Unterschied zwischen einer „Backdoor" und einem „Bot" zu kennen, ist in der IT-Sicherheit wertvolles Wissen. Lesen Sie daher die Definitionen in der folgenden Aufstellung:

- **Adware:** Software, die Werbebanner auf Webbrowsern (zum Beispiel Internet Explorer oder Mozilla Firefox) anzeigt.
- **Backdoor:** Anwendung, die externen Systemen den Zugang zum Computer ermöglicht.
- **Bot:** Ferngesteuerter *Trojaner,* der Zentralrechner im Internet infiziert; eine Gruppe von Bots wird als *Bot-Netz* bezeichnet.
- **Denial-of-Service-Angriff (DoS):** *Trojaner*, der den regulären Datenfluss in das und aus dem System unterbricht oder behindert und das System letztlich arbeitsunfähig macht. Jede Art von Schadprogrammen (Malware), die das normale Funktionieren eines Systems oder Netzwerkes unmöglich macht.
- **Keylogger:** *Spyware,* die die Eingaben an der Tastatur mitprotokolliert; oft verwendet, um Benutzernamen und Kennwörter zu sammeln.

- **Schadprogramm (Malware)**: Kurzbezeichnung für bösartige Software; darunter versteht man jede Art von bösartigem oder unerwartetem Programm oder Code.
- **Phishing**: Technik, bei der Benutzer durch seriös scheinende E-Mails auf betrügerische Weise dazu gebracht werden sollen, persönliche Angaben an eine gefälschte Internet-Seite zu übergeben.
- **Rootkit**: Eine Sammlung von Werkzeugen, mit der ein Hacker sein Eindringen verbergen und sich Zugang zu einem Netzwerk oder einem System verschaffen kann.
- **Spam**: Unerwünschte Werbe-Mail; kann Links zu bösartigem Code enthalten.
- **Spoofing:** Programmierung von Computern, um sich als jemand anderes auszugeben. Beim IP-Spoofing wird eine gefälschte IP-Adresse verwendet, um sich Zugang zu einem Netzwerk zu verschaffen.
- **Spyware**: Unerwünschte Software, die heimlich die Benutzeraktivität überwacht und in der Regel persönliche Daten mitprotokolliert und weitergibt.
- **Trojaner**: *Malware*, die harmlos erscheint, aber eine versteckte, böswillige Absicht hat.
- **Virus:** Code, der mit der Absicht geschrieben wurde, sich zu vervielfältigen. Ein Virus versucht, sich von Computer zu Computer zu verbreiten, indem er andere Dateien infiziert.
- **Computerwurm:** Spezielle Art von V*irus*, der in der Lage ist, Kopien von oder Teile von sich selbst über ein Netzwerk zu verbreiten.
- **Zero-day-Angriff:** *Malware,* die eine neu entdeckte Sicherheitslücke in einem System ausnutzt, noch bevor ein Patch (eine Nachbesserung) verfügbar ist.

Den durch Sicherheitslücken verursachten Beeinträchtigungen begegnen

Sicherheitslücken können für Ihr Unternehmen ein echtes Problem darstellen – von finanziellen Verlusten bis hin zur Schädigung des guten Rufes.

In kleinen Unternehmen liegen die durchschnittlichen Ausgaben für einen sehr schlimmen Zwischenfall zwischen 11.500 und 23.000 Euro. Das bedeutet aber, dass einige Unternehmen weit mehr verloren haben. Oftmals potenzieren sich die Auswirkungen in Kombination. Bei kleineren Unternehmen ist das schwerste Problem wohl die Stabilisierung der Betriebsabläufe bzw. die Produktivitätseinbußen.

Die Unterbrechung des täglichen Geschäftsbetriebs kann katastrophale Folgen haben. Stellen Sie sich nur einmal die folgenden Szenarien vor:

- Ihr Netzwerk ist ausgefallen oder Ihr Server funktioniert nicht richtig. Wie wirkt sich jede Stunde Produktivitätsverlust in finanzieller Hinsicht aus?
- Ihre Website fällt aus, und Sie verlieren die Bestellungen eines gesamten Tages. Wie groß ist der Schaden für Ihre Einnahmen bzw. Ihren guten Ruf?
- Ihre Mitarbeiter verbringen Zeit beim Surfen auf nicht geschäftsbezogenen Websites, wie z. B. Facebook und MySpace. Was kostet Sie das an verlorener Produktivität? Wie groß sind die Risiken für Ihr IT-System?

- Mitarbeiter können Ihrem guten Ruf unmittelbar schaden, indem sie Websites besuchen, auf denen sie sich aus rechtlicher Sicht nicht aufhalten dürfen. Das Verhalten Ihrer Mitarbeiter beim Surfen im Web kann indirekt eine Bedrohung für Ihr Unternehmen darstellen: Sie können Malware einschleusen, die einen Ihrer Computer infiziert. So kommt es zur Installation von Spyware oder einem *Bot-Netz*, das aus Ihrem Computer einen Host für Daten macht, die von entfernten Anwendern angesehen oder ausgetauscht werden.

Die Intensität schwerwiegender Vorfälle nimmt weiter zu. Es mag sein, dass die Anzahl der Vorfälle insgesamt zurück geht, aber es genügt eine Katastrophe, um Ihr gesamtes Unternehmen in den Ruin zu treiben.

Denken Sie an die versteckten Folgen von Sicherheitslücken. Oft handelt es sich bei den schwersten Problemen gerade um die, an die Sie nicht sofort denken. Dazu gehören zum Beispiel der Verlust einer entscheidenden Information, die Sie für den Abschluss eines Geschäftes brauchen, oder die Möglichkeit, dass Daten in die Hände eines Konkurrenten oder Kriminellen gelangen.

Überprüfen Sie Ihren Versicherungsschutz, und stellen Sie sicher, dass Sie gegen finanzielle Einbußen, die Sie durch eine schwerwiegende Sicherheitslücke erleiden können, versichert sind. Treffen Sie Maßnahmen zur Wiederherstellung des Unternehmens nach einer Katastrophe und zur Stabilisierung der Betriebsabläufe, damit Sie nach dem Sicherheitsvorfall so schnell wie möglich die Arbeit wieder aufnehmen können.

In den folgenden Abschnitten werden einige der durch Sicherheitslücken verursachten Auswirkungen beschrieben.

Ausfall des Computers, des Netzwerks oder der Website

So gut wie alle Sicherheitsvorfälle verursachen auf die eine oder andere Weise Ausfallzeiten. Ein schwerwiegender Zwischenfall kann einen Computer, ein Netzwerk oder einen Webserver vollständig außer Betrieb setzen. Selbst durch ein weniger schwerwiegendes Problem, wie zum Beispiel einen *Denial-of-Service-Angriff* (ein Versuch, Benutzer daran zu hindern, auf ein System oder Netzwerk zuzugreifen), kann Ihr Netzwerk fast zum Erliegen kommen.

Der richtige Zeitpunkt kann hier von entscheidender Bedeutung sein. Niemand kann die Gesamtkosten einer Ausfallzeit beziffern, wenn Ihr Computer außer Gefecht gesetzt wird, während Sie an einer Verkaufstaktik für eine neue Geschäftsidee arbeiten. Das Gleiche gilt, wenn Ihre Website nicht verfügbar ist und ein Kunde eine Bestellung aufgeben oder eine Anfrage stellen will. Dieser Kunde kommt vielleicht nie mehr zurück.

Eine Verlangsamung Ihres Systems stellt die Wirksamkeit all Ihrer Notfallpläne auf die Probe. Wenn Sie jedoch zuverlässige Maßnahmen zur Wiederherstellung des Unternehmens und zur Stabilisierung der Betriebsabläufe getroffen haben, können Sie verlorene Daten wiederherstellen oder auf ein zusätzlich verfügbares Gerät bzw. Netzwerk umschalten und so weiterarbeiten, als ob nichts passiert wäre.

Beschädigung, Zerstörung und Diebstahl von Daten

Es wird Ihnen vielleicht nicht bewusst sein, aber die meisten Unternehmen sind darauf angewiesen, dass Daten richtig funktionieren. Ob Sie es mögen oder nicht, Daten halten die Unternehmen am Laufen – angefangen bei Kundennamen und Adressen über das geistige Eigentum, das Ihre Produkte und Services einzigartig macht, bis zu den täglichen Routinearbeiten der Buchhaltung. Sollten diese vertraulichen Daten beschädigt, zerstört oder gestohlen werden, kann Ihnen das schlaflose Nächte bereiten.

Der Diebstahl von Kundendaten hat katastrophale Folgen. Wie oft hat ein Vertriebsmitarbeiter eine Firma verlassen und die größten Kunden mitgenommen? Oder im Falle von geistigem Eigentum: In nicht wenigen Fällen hat ein Geschäftsführer ein Unternehmen verlassen, um ein anderes zu gründen, dessen Geschäftstätigkeit dann aber erstaunliche Ähnlichkeit zum ersten Unternehmen aufwies. Unvollständige oder fehlende Daten können gleichermaßen schädlich sein, und in der Regel wird das Fehlen erst in der Verwaltung bemerkt oder dann, wenn Rechte aus einem Vertrag geltend gemacht werden sollen.

Größere Unternehmen verfügen über angemessene Schutzmechanismen, die verhindern, dass so etwas passiert. Bei kleineren Unternehmen sind diese Vorfälle aber fast schon an der Tagesordnung.

Den neuesten Forschungsergebnissen der TrendLabs zufolge ist datenstehlende Malware heute eine der am schnellsten anwachsenden Bedrohungskategorien. Es gibt viele verschiedene Arten, und es kann sein, dass Sie nicht einmal wissen, dass sie sich in Ihrem System befindet. Das Hauptziel von Malware ist es, sensible Daten auf den Computern der Benutzer zu sammeln und an die kriminellen Betreiber zurückzusenden, entweder zur direkten Verwertung oder zum Weiterverkauf auf dem Schwarzmarkt.

Wiederherstellung nach Identitäts- und Kennwortdiebstahl

Jeder kennt die Gefahren von Identitätsdiebstahl im privaten Umfeld, aber vielleicht ist Ihnen nicht bewusst, dass dies im Unternehmensbereich genauso schwerwiegende Folgen hat. So können sich Betrüger durch den Diebstahl von Kennwörtern und Zugangscodes als leitende Firmenmitarbeiter ausgeben.

Da Unternehmenskonten in der Regel auf Kredit laufen, können Betrüger, die sich als Geschäftsführer ausgeben, oft beträchtliche Schulden anhäufen, bevor sie entdeckt werden. Muss dann am Monatsende die Rechnung bezahlt werden, erlebt das Unternehmen eine böse Überraschung. Bei 88 Prozent der schwersten Sicherheitsverletzungen gab es keine finanziellen Einbußen. Aber liegt das vielleicht daran, dass die Firmen die Augen vor der Wahrheit verschließen?

Der Online-Sicherheitsgruppe Get Safe Online zufolge kann der Diebstahl der Unternehmensidentität viele Formen annehmen. Dazu zählt unter anderem, wenn:

- jemand ein Geschäftskonto auf den Namen Ihres Unternehmens eröffnet und anschließend zahlreiche Einkäufe mit gestohlenen Kreditkarten akzeptiert, die Einnahmen aber auf seinem eigenen Bankkonto deponiert. Wenn sich dann die Beschwerden häufen und das Kreditkartenunternehmen von Ihnen die Rückverrechnung einfordert, sind die Diebe längst über alle Berge.
- jemand Papierkörbe durchwühlt auf der Suche nach Namen von Mitarbeitern, nach Bankverbindungen und anderen sensiblen Daten.
- jemand mit gestohlener Kreditkarte in Ihrem Online-Shop oder telefonisch unter Angabe einer falschen Kontoverbindung Waren bestellt (und dabei den Anschein erweckt, es handle sich um ein seriöses Unternehmen).
- jemand Ihre Website hackt, um dort gefälschte oder schädliche Daten zu verbergen, oder die Website vollständig unter seine Kontrolle bringt, um darüber pornografisches Material zu verteilen.

- jemand datenstehlende Malware verwendet, um Ihren Benutzernamen und Ihr Kennwort für das Online-Banking zu erfahren und Ihre Gelder auf ein anderes Konto zu verschieben.

Laut Studie zum Identitätsdiebstahl und -missbrauch im Internet, die auf Initiative des Bundesministeriums des Innern (BMI) und im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik (BSI) 2010 veröffentlicht wurde, entstehen für die deutsche Wirtschaft pro Jahr Schäden in Milliardenhöhe durch Identitätsbetrug. Gesicherte Zahlen fehlen noch.

Mit Finanzdiebstahl konfrontiert

Eigentlich komm es eher selten vor, dass von Finanzdiebstahl in Unternehmen berichtet wird. Allerdings fand die 2008 durchgeführte Studie zu Informationssicherheitslücken heraus, dass bei den schwerstwiegenden Sicherheitsverletzungen nur in 12 Prozent der Fälle finanzielle Einbußen zu verzeichnen waren. Es kann jedoch sein, dass diese relativ niedrige Zahl darauf zurückzuführen ist, dass die Unternehmen interne Diebstähle unter Ausschluss der Öffentlichkeit klären oder ansonsten die Augen vor der Wahrheit verschließen – schließlich gibt keiner gerne zu, dass er um sein Geld gebracht wurde.

Wenn man allerdings das Thema Sicherheitslücken aus einem anderen Blickwinkel heraus betrachtet, stellt man fest, dass die meisten Angriffe heutzutage finanzielle Beweggründe haben und aus Profitgier erfolgen. Wenn es also nicht Ihr Unternehmen ist, das Geld verliert, kann es sein, dass jemand anderes zu einem späteren Zeitpunkt den Preis dafür zahlen muss.

Die Kosten der Reaktion auf einen Sicherheitsvorfall erklären

Die Reaktion auf einen Sicherheitsvorfall kann ziemlich teuer werden, und es ist gar nicht so einfach, alle Kosten abzuschätzen.

Zu den Kostenfaktoren, an die Sie vielleicht nicht unmittelbar denken, gehören unter anderem:

- **Arbeitsausfälle:** Da die Mitarbeiter für die meisten Unternehmen den größten Kostenfaktor darstellen, ist der Ausfall der Arbeitskräfte die gravierendste Auswirkung des Vorfalls. Dabei geht es nicht nur um die Zeit der Mitarbeiter, die das Betriebssystem neu installieren bzw. die Daten wiederherstellen. Nicht zu vergessen sind die Kosten, die entstehen, weil Ihre Mitarbeiter während der Systemwiederherstellung nicht weiterarbeiten können.
- **Verpasste Chancen:** Zeit ist Geld in der Geschäftswelt. Berücksichtigen Sie daher auch die *Einbußen durch verpasste Chancen:* Potenzielle Einnahmen, die Sie hätten erwirtschaften können, hätte sich Ihr Unternehmen nicht gerade von einem Vorfall erholen müssen.

Unternehmen geben im Durchschnitt zwischen 1.150 und 2.300 Euro aus, um nach den schlimmsten Vorfällen wieder auf die Beine zu kommen – und das zusätzlich zu den Personalkosten.

Ihr guter Ruf erleidet erheblichen Schaden

Eine der wichtigsten immateriellen Folgen von Sicherheitsverletzungen ist der Schaden, den Ihr Unternehmen in den Augen Ihrer Kunden nimmt. Kunden und Partner kümmert es wahrscheinlich wenig, dass Sie mit einer Sicherheitsverletzung beschäftigt waren; für sie ist nur interessant, dass sie von Ihnen nicht den erwarteten Service erhalten haben. Kunden, Geschäftspartner und Investoren sehen Sie daraufhin eventuell als erhöhtes Risiko an.

Außerdem kann es sein, dass Ihre Mitarbeiter die Ausfallzeiten als unnötig wahrnehmen. Dies wiederum wirkt sich negativ auf ihr Engagement und ihre Produktivität aus.

Als kleineres Unternehmen denken Sie vielleicht, dass ein Sicherheitsvorfall Ihrem guten Ruf nicht schaden wird. Wenn sich ein Kunde allerdings unsicher ist, ob er mit einem kleineren Lieferanten zusammenarbeiten soll, wird das regelmäßige Auftreten von Zwischenfällen seine Unsicherheit nur noch verstärken – er wird sich also eher an ein größeres Unternehmen wenden, das in der Lage ist, mit solchen Störungen umzugehen.

Die Bedrohung für Ihr Unternehmen einschätzen

Es ist ganz klar, dass IT-Bedrohungen nicht die gleichen Auswirkungen auf alle Unternehmen haben. Für ein neu gegründetes High-Tech-Unternehmen mit vielen digitalen Vermögenswerten liegt die Herausforderung darin, seine IP-(Internet Protocol)-Kommunikation zu schützen und seinen guten Ruf sowie die Beziehungen zu Lieferanten und Kunden zu pflegen. Bei einem eher traditionellen Unternehmen, wie zum Beispiel einem Taxiunternehmen, geht es in Sachen IT-Sicherheit eher darum, die Computer im Netzwerk und die Kommunikationsinfrastruktur des Unternehmens zu administrieren.

Einige Bedrohungen sind allgegenwärtig: Der Diebstahl von Computerzubehör trifft jedes Unternehmen, da es Geld kostet, die gestohlenen Geräte zu ersetzen. Aber ss lohnt sich, darüber nachzudenken, welche spezifischen Schwachstellen Ihr Unternehmen aufweist und welchen konkreten Auswirkungen eine Bedrohung für Sie haben könnte. Verschaffen Sie sich mit Tabelle 1-1 einen Überblick über die gravierendsten Bedrohungen, die in der oberen Zeile von links nach rechts aufgeführt sind. Haken Sie dann die Schwachstellen ab (in der Liste von oben nach unten aufgeführt), mit denen Ihr Unternehmen konfrontiert ist. Ein Haken steht also für einen Bereich, in dem eine gravierende Bedrohung Ihr Unternehmen beeinträchtigen würde

	Systemausfall	Infektion durch Virus/Malware	Missbrauch durch Personal	Unberechtigter Zugriff	Physischer Diebstahl	Computer-diebstahl	Informations-diebstahl
Website	✓	✓		✓	✓		
Vertrauliche Daten				✓	✓		✓
Wichtige Komm.–Infrastruktur	✓				✓		
Missions-kritische Verarbeitung	✓	✓	✓	✓	✓	✓	✓
E-Mail–Komm.	✓						
Sonstiges							

Tabelle 1-1: Schwachstellen und Bedrohungen überprüfen

Eine Risikobewertung durchzuführen, bei der sich ein unabhängiger Dritter einen Überblick über die Schwachstellen Ihrer IT-Infrastruktur verschafft und mögliche Risiken ermittelt, lohnt sich auf jeden Fall. Einige Anbieter tun dies gegen einen geringen Aufpreis - in der Hoffnung, weiter beauftragt zu werden. Da jede Infrastruktur anders ist, lohnt es sich, besagte Bewertung von einem Fachmann durchführen zu lassen; möglicherweise sind Sie von den Ergebnissen überrascht.

Ein Blick auf gesetzliche Anforderungen

Es gibt eine Reihe von Gesetzen, die Sie im Hinterkopf behalten müssen, wenn es um Ihre Haftung in Sachen IT-Sicherheit geht. Grundsätzlich muss Ihr Unternehmen rechtliche Anforderungen hinsichtlich der IT-Sicherheit, des Datenschutzes, der elektronischen Kommunikation sowie aufgrund des Arbeitsrechts berücksichtigen. Außerdem müssen Sie eine Reihe von Bestimmungen der Europäischen Union beachten.

Datenschutz respektieren

Die Anforderungen an ein Unternehmen bei der Verarbeitung personenbezogener Daten sind im Bundesdatenschutzgesetz (BDSG) geregelt. § 9 BDSG regelt technische und organisatorische Maßnahmen, die Unternehmen zu treffen haben. Folgende Maßnahmen sind näher beschrieben:

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Datentrennung

Das Gesetz sieht auch vor, dass der Betroffene Auskunft über die zu seiner Person gespeicherten Daten verlangen kann. Zusätzlich definiert die EU-Datenschutzrichtlinie für elektronische Kommunikation (die auch in Deutschland umgesetzt worden ist), wie bei unerbetenen Nachrichten über Telefon, Fax, E-Mail und SMS zu verfahren ist. Falls Sie Werbeanrufe tätigen, Werbefaxe oder Werbe-E-Mails versenden wollen, brauchen Sie eine vorherige ausdrückliche Einverständniserklärung des Kunden. Allerdings ist das Versenden von Werbe-E-Mails für eigene ähnliche Waren oder Services gestattet, wenn Sie die E-Mail-Adresse in Zusammenhang mit einer Geschäftsbeziehung erhalten haben. Der Kunde muss die Möglichkeit erhalten, der E-Mail-Werbung zu widersprechen. Diese Datenschutzrichtlinie reguliert auch die Verwendung von Cookies, den kleinen Textdateien, die beim Besuch einer Website im System eines Benutzers gespeichert werden.

Haftung gegenüber Mitarbeitern und Dritten

Es gibt eine Reihe von Bestimmungen, die die Haftung von Unternehmen gegenüber ihren Mitarbeitern und Dritten betreffen. Hierzu gehören unter anderem:

- Bundesdatenschutzgesetz
- Telekommunikationsgesetz, das das Fernmeldegeheimnis schützt und u.a. das Abhören von Gesprächen verbietet
- Strafgesetzbuch, das etwa die Computersabotage, das Ausspähen von Daten und die rechtswidrige Datenveränderung unter Strafe stellt

Die Reaktion der Sicherheitsbranche

In den Anfängen der IT-Sicherheit konzentrierten sich die Anbieter auf einen einzelnen Bereich, wie zum Beispiel Antiviren-Software oder Firewalls, und ließen andere Bereiche außer Acht. Allerdings fängt die Branche jetzt an, ihre Aktivitäten abzurunden, da die Unternehmen einsehen, dass ein koordiniertes Verteidigungssystem gegen die Angriffe auf die Informationssicherheit nötig ist.

Firewalls und Anti-Malware-Technologien sind heute ausgereifter und werden zusammen mit anderer Funktionalität, wie z. B. Anti-Spam- und Anti-Spyware-Technologie, in Suites gebündelt. Die *Endpunkt-Sicherheit,* die sich ausschließlich auf den Computer oder ein anderes Gerät am Benutzerende konzentriert, wird bewusst durch einige Funktionen der *Gateway-Sicherheit* (Sicherheitslösung vor der Verbindung mit dem Internet) erweitert. Ziel ist es, Internet-Bedrohungen abzuwehren, bevor sie ihr Ziel erreichen. Die Tendenz geht also dahin, sowohl das Gateway als auch den Endpunkt mit einer Lösung zu schützen.

Das Aufkommen von Hosted Security Services ist eine weitere willkommene Entwicklung für kleine Unternehmen. Dadurch verringern sich die IT-Ausgaben – sowohl für Hardware als auch Verwaltung– und die Services sind verlässlicher, da sich Elemente der Sicherheitslösung auf den Servern des Sicherheitsanbieters befinden. Mehr dazu im nächsten Kapitel.

Sie glauben vielleicht, dass die Sicherheitsservices bei Ihnen vor Ort ausgeführt werden müssen, doch viele Unternehmen nutzen bereits Hosted Services in Form von Webmail oder CRM (Customer Relationship Management) und wickeln vielleicht ihre Gehaltszahlungen über ein externes Büro ab. Es spricht vieles dafür, einen Hosted Security Service zu nutzen – wer die Software entwickelt hat, kann sie auch am besten ausführen. Außerdem verfügen die Anbieter über Rechenkapazitäten, von denen Sie nur träumen können.

Das Pay-as-you-go-Verfahren ist außerdem ein vorhersehbarer monatlicher Posten in Ihrer Bilanz. Sie müssen sich keine Gedanken um die Kosten zukünftiger Upgrades machen, während sich die IT-Sicherheit weiter entwickelt.

Kapitel 2

Am Anfang steht die Sicherheitsrichtlinie

In diesem Kapitel

- Lernen Sie, warum eine Sicherheitsrichtlinie notwendig ist
- Werfen wir einen Blick auf Normen und bewährte Methoden
- Beschäftigen wir uns mit der Sicherheitsverwaltung
- Lernen Sie, technische Kontrollen zu implementieren

Nachdem Sie nun die Bedrohungen erkannt haben und sich den Grundsätzen guter IT-Sicherheit (siehe Kapitel 1) verpflichten, ist die nächste Frage wahrscheinlich: Wo fange ich an? Wenn Sie sich bereits mit den Risiken für Ihr Unternehmen beschäftigt haben, ist der erste Schritt jetzt, eine Sicherheitsrichtlinie zu entwickeln und Ihre Mitarbeiter darüber zu unterrichten.

Im nächsten Schritt überlegen Sie sich, wie Sie die Richtlinie mit der bereits vorhandenen Technologie durchsetzen, um Sicherheitsrisiken zu überwachen und mögliche Lücken zu schließen. Die Technologie ist allerdings nur ein Teil des Ganzen – der andere Teil sind die Menschen, die Abläufe und die Richtlinien.

Das Kapitel streift auch die Frage, welche Best Practices große Unternehmen bzw. Konzerne nutzen, und was wir eventuell daraus lernen können.

Eine Sicherheitsrichtlinie abfassen

Eine Sicherheitsrichtlinie ist für ein Unternehmen die Grundlage, auf der gute IT-Sicherheit aufbaut. Unter einer *Sicherheitsrichtlinie* versteht man eine Absichtserklärung dazu, wie Sie Ihre digitalen Vermögenswerte schützen und Ihr Unternehmen überwachen wollen. Die Sicherheitsrichtlinie dient als zentrale Informationsquelle für die Unternehmensleitung, die Mitarbeiter und Dritte. Sie beinhaltet die Unternehmensleitung alles Wesentliche: Vorgänge und Maßnahmen, Funktionen und Verantwortungsbereiche der einzelnen Personen, eine Beschreibung der eingesetzten technischen Maßnahmen und wie das Unternehmen nach einem Sicherheitsvorfall wiederhergestellt wird.

Ihre Sicherheitsrichtlinie basiert auf der im vorherigen Kapitel skizzierten Risikoanalyse und Ihrer Kenntnis der gravierendsten Bedrohungen, mit denen Sie konfrontiert sind.

Um sicherzustellen, dass die Sicherheitsrichtlinie verbindlich ist, sollte sie von der Geschäftsleitung genehmigt und an sich verändernde Situationen zeitnah angepasst werden. Es muss nicht bei jedem Punkt ins Detail gegangen werden, aber sehen Sie die Sicherheitsrichtlinie als einen Aktionsplan, der die gefährdeten Informationsressourcen und die für sie beabsichtigten Schutzmaßnahmen zusammenfasst.

Am besten wäre es, wenn Sie beim Zusammenstellen der Sicherheitsrichtlinie schrittweise vorgehen. Das bedeutet, dass Sie mit einem Mission Statement auf höchster Ebene beginnen und sich dann nach unten auf die Ebene der physischen Geräte, Funktionen und Verantwortungsbereiche der Mitarbeiter vorarbeiten. Dazu gehören auch Hinweise zur akzeptablen Nutzung durch Mitarbeiter, wie bei Verstößen verfahren wird usw. Hier können Sie auch Ihre Pläne zur Stabilisierung des Betriebsablaufs und zur Wiederherstellung nach einem Vorfall festhalten.

Was gehört hinein?

Je nach Unternehmen sind die Sicherheitsrichtlinien sehr verschieden, aber ganz grundsätzlich sollte jede Richtlinie die folgenden Punkte beinhalten:

- Eine klare Erläuterung hinsichtlich des Zwecks der Richtlinie, einschließlich der obersten Ziele und der strategischen Bedeutung, die die Informationssicherheit für das Unternehmen hat.
- Eine Erklärung der Geschäftsleitung, dass sie diese Richtlinie unterstützt und dadurch ihr Engagement in Sachen Informationssicherheit verdeutlicht.
- Die verfügbaren Schulungsmaßnahmen, die den Mitarbeitern helfen, die Informationssicherheit und die Risiken zu verstehen.
- Eine Erläuterung der Mindestsicherheitsstandards, wobei die Maßnahmen hervorgehoben werden, denen in Bereichen von besonderer Bedeutung für den Geschäftsbetrieb Folge zu leisten ist. Zum Beispiel sollte jede Sicherheitsrichtlinie elementare Sicherheitsvorkehrungen in Bezug auf Computerviren zusammenfassen sowie Leitfäden zum Surf-Verhalten und Anweisungen für die Erstellung von Kennwörtern geben.
- Definitionen der Funktionen und Verantwortungsbereiche innerhalb des Unternehmens für die Informationssicherheit.
- Die Abläufe für das Berichten von, das Reagieren auf und die Behebung von Sicherheitsvorfällen.
- Die Pläne zur Stabilisierung des Betriebsablaufs, die erläutern, wie die Geschäftstätigkeit im Falle einer Naturkatastrophe, wie zum Beispiel Feuer oder Überschwemmung, weitergeführt wird.
- Verweise auf ergänzende Unterlagen, wie zum Beispiel Mitarbeiterrichtlinien, Maßnahmen, Leitfäden oder Sicherheitsspezifikationen und -standards. Wollen Sie zum Beispiel näher auf die Einzelheiten einer Internet-Richtlinie eingehen, könnten Sie folgende Punkte mit einschließen:
    - Die Nutzung des Internets für das Unternehmen und daraus resultierende Bedrohungen.
    - Die zulässigen und die gesperrten Internet-Services.
    - Die für das Zulassen von Internet-Verbindungen zuständige(n) Person(en).
    - Die für die IT-Sicherheit verantwortliche(n) Person(en).

- Die Standards, Leitfäden und Best Practices, die zu befolgen sind.

Eines der schwächsten Glieder in der Sicherheitskette eines Unternehmens ist oft der Kennwortschutz, da die Benutzer z. B. ihre Kennwörter auf einer Haftnotiz neben dem Computer notieren oder das Standardkennwort nicht abändern. Stellen Sie also sicher, dass Ihre Sicherheitsrichtlinie vor einem solch riskanten Verhalten warnt und sichere Protokolle für den Kennwortschutz festlegt.

Wollen Sie noch einen Schritt weiter gehen, so können Sie als einen Teil der Sicherheitsrichtlinie *allgemeine Nutzungsbedingungen* aufstellen, die einen Überblick darüber geben, was das Unternehmen als zulässig bzw. unzulässig erachtet. Mehr dazu im nächsten Abschnitt.

Vielleicht möchten Sie auch separate allgemeine Nutzungsbedingungen sowohl für den Internet-Zugang und die Unternehmens-E-Mails als auch für die Verwendung von IT-Vermögenswerten anderer Unternehmen erstellen. Im nächsten Abschnitt befassen wir uns mit solchen allgemeinen Nutzungsbedingungen.

Machen Sie hinsichtlich der Bedingungen und Maßnahmen nicht zu viele Vorschriften für die einzelnen IT-Vermögenswerte. Ihre Sicherheitsrichtlinie dient vorrangig dazu, Ihren Mitarbeitern die Gesamtziele aufzuzeigen, ihnen klar zu machen, warum bestimmte Maßnahmen getroffen wurden und was die Folgen sind, wenn diese Maßnahmen nicht eingehalten werden.

Akzeptable Nutzung definieren

Der Schutz Ihrer IT-Vermögenswerte beginnt damit, dass Ihre Mitarbeiter eindeutig formulierte Handlungsanweisungen zur akzeptablen Nutzung, zur Vertraulichkeit und zu den Standards bezüglich der Sicherheitsmaßnahmen erhalten. Die *allgemeinen Nutzungsbedingungen* machen klar, was während der Arbeitszeit und auf Firmencomputern erlaubt bzw. nicht erlaubt ist, und sie weisen auf die Folgen hin, wenn gegen die Richtlinie verstoßen wird.

Ohne eindeutige Handlungsanweisungen kann es vorkommen, dass die Mitarbeiter das Unternehmen schädlicher Software

aussetzen, dass sie vertrauliche Informationen über das Internet mitteilen oder dass sensible Daten über Laptops oder USB-Sticks außer Haus gelangen.

Es kann sein, dass einige Mitarbeiter diese allgemeinen Nutzungsbedingungen als drakonisch empfinden. Versuchen Sie, einen Mittelweg zwischen Pragmatismus und Kontrolle zu finden. Wenn Ihr Unternehmen klarstellt, welche konkreten Risiken vermieden werden sollen, werden die Mitarbeiter einsehen, dass Nutzungsbedingungen wichtig sind. Beteiligen Sie die Mitarbeiter an der Ausarbeitung der Richtlinien, dann gewinnen Sie vom ersten Tag an ihre Unterstützung. Außerdem sollten Sie Ihre Mitarbeiter ermutigen, Ihnen Rückmeldung zu geben, ob bestimmte Einschränkungen funktionieren und praktikabel sind oder nicht.

Durch die Verknüpfung der allgemeinen Nutzungsbedingungen mit den Arbeitsverträgen und Disziplinarmaßnahmen (Betriebsbußen) werden die Mitarbeiter auf diese Weise in der Unternehmenskultur zusammengeschweißt.

Surfen im Internet, ohne das Unternehmen zu gefährden

Ihre Arbeitnehmer sind zwar auf das Internet angewiesen, um ihre Arbeit zu verrichten, aber das Internet kann die Produktivität auch verringern – und tut dies auch. Zugleich ist Ihr Unternehmen dadurch verschiedenen, über das Internet übertragenen Bedrohungen ausgesetzt.

Im Folgenden finden Sie Vorschläge, die Sie in eine Internet-Richtlinie mit aufnehmen können:

- Die Nutzungszeiten, in denen eine private Nutzung des Internets gestattet bzw. nicht gestattet ist. Wenn Sie zum Beispiel nicht wollen, dass Ihre Mitarbeiter während der Arbeitszeiten Facebook besuchen, sollten Sie dies hier festlegen.
- Rechtswidrige Inhalte wie pornografisches Material, obszöne Inhalte oder Inhalte, die zur Volksverhetzung aufstacheln usw.
- Der Umgang mit vertraulichen Daten – zum Beispiel, dass diese nicht außerhalb des Intranets zugänglich gemacht werden dürfen.
- Vorschläge für den Umgang mit Firmeneigentum, wie zum Beispiel Laptops.

- Handlungsanweisungen zum Herunterladen und Installieren von Software.
- Sicherheitsrichtlinien, wie zum Beispiel die Sicherheitseinstellungen des Browsers.
- Ein Verbot für das Verbreiten oder Herunterladen urheberrechtlich geschützten Materials.
- Genaue Angaben zu allen Überwachungsaktivitäten, die das Unternehmen eingerichtet hat.
- Die Folgen bei Verstoß gegen die Richtlinie.

Wie wird dies durchgesetzt? Ein Programm zum Filtern von Websites kann dabei helfen, einige Probleme zu verhindern oder aufzudecken.

Vorlage für allgemeine Nutzungsbedingungen

Dieser Textvorschlag legt allgemeine Nutzungsrichtlinien für die Internet-Verwendung dar. Sie können ihn kopieren und unter Berücksichtigung der rechtlichen Anforderungen, die für Ihr Unternehmen gelten, an Ihre Bedürfnisse anpassen. Falls in Ihrem Unternehmen ein Betriebsrat besteht, prüfen Sie, inwieweit diese Nutzungsrichtlinie der Mitbestimmung des Betriebsrates unterliegt.

Die Nutzung des Internets von den Mitarbeitern von [Name des Unternehmens] ist gestattet und wird gefördert, wenn die Nutzung die Zwecke und Zielvorgaben des Unternehmens unterstützt. [Name des Unternehmens] hat dennoch eine Richtlinie für die Nutzung des Internets erstellt, wobei die Mitarbeiter sicherstellen müssen, dass sie:

- *die geltenden Rechtsvorschriften einhalten,*
- *das Internet in akzeptabler Weise nutzen,*
- *kein unnötiges Geschäftsrisiko für das Unternehmen schaffen, indem sie das Internet missbrauchen.*

Unzulässiges Verhalten

Insbesondere die folgenden Punkte werden als unzulässige Nutzung bzw. unzulässiges Verhalten seitens der Mitarbeiter angesehen:

- *Der Besuch von Websites mit obszönen, volksverhetzenden, pornografischen oder anderweitig illegalen Inhalten.*

(Fortsetzung)

(Fortsetzung)

- *Die Nutzung des Computers für jegliche Form von Betrug oder das Erstellen von Raubkopien von Software, Film und Musikdateien.*
- *Die Nutzung des Internets zum Versenden anstößiger oder belästigender Inhalte an andere Nutzer.*
- *Das Herunterladen von Software oder urheberrechtlich geschützter Materialien Dritter, sofern diese Software nicht durch einen Vertrag oder eine andere Lizenz abgedeckt und deren Nutzung gestattet ist.*
- *Unerlaubtes Eindringen in unbefugte Bereiche*
- *Das Veröffentlichen diffamierender bzw. wissentlich falscher Inhalte über [Name des Unternehmens], Ihre Kollegen bzw. Kunden in Kontaktnetzwerkseiten, Blogs, Wikis und anderen öffentlichen Online-Formaten.*
- *Das Durchführen von Aktivitäten, die die Arbeitszeit von Mitarbeitern und vernetzten Ressourcen verschwenden.*
- *Das Einschleusen jeglicher Form bösartiger Software in das Unternehmensnetzwerk.*

Firmeneigene Informationen, die auf Seiten Dritter gespeichert sind

Wenn Sie während der Arbeitszeit geschäftsrelevante Daten erstellen, erheben oder bearbeiten, bleiben diese Informationen Eigentum von [Name des Unternehmens]. Hierzu gehören Daten, die auf Websites Dritter gespeichert sind, einschließlich Webmail-Service-Providern und Kontaktnetzwerken, wie zum Beispiel Facebook und LinkedIn.

Überwachung

[Name des Unternehmens] stimmt zu, dass die Nutzung des Internets ein wertvolles Arbeitsmittel ist. Allerdings kann sich der Missbrauch dieser Einrichtung negativ auf die Produktivität der Mitarbeiter und den guten Ruf des Unternehmens auswirken.

Außerdem werden alle webbasierten Ressourcen des Unternehmens für geschäftliche Zwecke zur Verfügung gestellt. Daher behält sich das Unternehmen das Recht vor, den Umfang des Internet- und Netzverkehrs sowie die besuchten Websites im Rahmen der gesetzlichen Vorgaben zu überwachen. Der genaue Inhalt bestimmter Vorgänge wird nicht überwacht, es sei denn, es liegt ein Verdacht auf Missbrauch vor und die Überwachung ist gesetzlich zulässig.

Sanktionen

In den Fällen, in denen angenommen wird, dass ein Mitarbeiter gegen diese Richtlinie verstoßen hat, werden arbeitsrechtliche Maßnahmen gegen diesen Mitarbeiter eingeleitet. Falls festgestellt wird, dass der betreffende Mitarbeiter gegen die Richtlinie verstoßen hat, erhält der Mitarbeiter eine Betriebsbuße, die

von einer mündlichen Verwarnung bis hin zur Entlassung gehen kann. Die tatsächlich angewendete Betriebsbuße richtet sich zum Beispiel nach der Schwere des Verstoßes und den Eintragungen in der Personalakte des Mitarbeiters.

***Anmerkung:** Die Betriebsbußen sollten speziell auf Ihr Unternehmen zugeschnitten sein und die normalen betrieblichen Abläufe und Betriebsbußen im Rahmen der arbeitsrechtlichen Anforderungen wiedergeben. Setzen Sie die Betriebsbußen von Anfang an fest, und nehmen Sie sie in die allgemeinen Nutzungsbedingungen mit auf.*

Einverständnis

Alle Mitarbeiter des Unternehmens, Auftragnehmer und Aushilfskräfte, die berechtigt sind, den Internet-Zugang des Unternehmens zu nutzen, müssen diese allgemeinen Nutzungsbedingungen unterschreiben, wobei sie bestätigen, dass sie diese Richtlinie verstehen und akzeptieren.

Richtlinie zum Versenden von E-Mails

E-Mails sind mittlerweile die häufigste Methode für den Versand geschäftlicher Kommunikation. Daher müssen Sie die Mitarbeiter auf die Sicherheitsmaßnahmen aufmerksam machen und sicherstellen, dass sie befolgt werden. Einige Aspekte, mit denen Sie sich in diesem Zusammenhang befassen müssen:

- Die Verwendung einer rechtlichen Klarstellung in den E-Mails („Diese E-Mail ist eine private Mitteilung und stellt nicht die Ansichten des Arbeitgebers dar ...“).
- Handlungsanweisungen zum Öffnen und Anzeigen von E-Mail-Anhängen.
- Falls nötig, zusätzliche Handlungsanweisungen in Bezug auf den Datenschutz, den Fernabsatz und Beleidigungsdelikte.
- Den Umgang mit vertraulichen Daten, die per E-Mail gesendet werden, und in welchen Fällen eine Verschlüsselung gemäß den Unternehmensrichtlinien notwendig ist.

Sicherstellen, dass die Richtlinie funktioniert

Zu viele Sicherheitsrichtlinien verstauben auf Regalen oder liegen unbeachtet und unbeliebt auf der Festplatte eines

Computers. Was dabei der entscheidende Punkt ist: Sie werden nicht durchgesetzt. Damit eine Sicherheitsrichtlinie auch Sinn macht, muss sie ein regelmäßig genutztes Dokument sein, auf das die Geschäftsleitung und die Mitarbeiter zugreifen und auf das sie sich beziehen können.

Machen Sie Ihre Mitarbeiter auf die Sicherheitsrichtlinie aufmerksam und sorgen Sie dafür, dass alle Beteiligten stets über die Inhalte informiert sind. Durch sichtbares Engagement für die Durchsetzung und kontinuierliche Aktualisierung der Richtlinie gibt die obere Führungsebene dem Thema zusätzliches Gewicht und steigert die Akzeptanz im Unternehmen.

Der soziale Konsens in Bezug auf eine zulässige Nutzung kann sich natürlich mit der Zeit ändern, und auch die verfügbaren Internet-Services entwickeln sich weiter und verändern sich. Sorgen Sie daher für eine regelmäßige Überprüfung Ihrer Sicherheitsrichtlinie, damit die in ihr enthaltenen Informationen stets zutreffend sind – ein Richtliniendokument, das einen vom Unternehmen nicht mehr unterstützten Webbrowser voraussetzt, macht das gesamte Dokument wenig effektiv.

Best Practices analysieren

Die ISO-Norm ISO 27001 stellt einen Gold-Standard der Informationssicherheitsmanagements dar. Wenn Sie diese Norm einhalten, profitieren Sie von Einsichten, die sich über Jahre hinweg entwickelt haben, und von praktischer Erfahrung, wie man am besten ein Verwaltungssystem für Informationssicherheit aufbaut und führt.

Für die meisten kleinen Unternehmen ist es wahrscheinlich zu mühsam, ihr Verwaltungssystem zu zertifizieren. Es sei denn, Sie sind in einer Branche tätig, in der Sie großes Interesse daran haben, den Kunden Ihre Informationssicherheit durch Referenzen unter Beweis zu stellen. Allerdings kann jeder von den Normanforderungen profitieren, von denen Sie viele in diesem Buch finden.

Wenn Sie Hilfe bei der Ausarbeitung einer Richtlinie oder der Einrichtung einer IT-Sicherheitsinfrastruktur benötigen, finden Sie zahlreiche Informationen und Hilfestellung bei verschiedenen Industrieverbänden und Sicherheitsanbietern, wie zum Beispiel denjenigen in der Linkliste.

Weitere Quellen

- BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (www.bitkom.de) bietet eine Reihe von Orientierungshilfen zum Thema IT-Sicherheit.
- Als nationale Sicherheitsbehörde ist es das Ziel des Bundesamtes für Sicherheit in der Informationstechnik (BSI), die IT-Sicherheit in Deutschland voran zu bringen. Unter www.bsi.de erhalten Sie aktuelle Informationen zu Themen rund um die IT-Sicherheit.
- Get Safe Online (www.getsafeonline.org), eine Partnerschaft zwischen der britischen Regierung und Industriepartnern, beinhaltet detaillierte Ratschläge für kleine Unternehmen auf Englisch.
- Trend Micro (www.trendmicro.de) stellt eine Vielzahl weiterer Informationsquellen zur Verfügung.

Die Sicherheitsrichtlinie verwalten

Nachdem Sie eine Bewertung der für Ihr Unternehmen einschlägigen Risiken durchgeführt und auf dieser Basis eine Sicherheitsrichtlinie definiert haben, müssen Sie entscheiden, wie die Sicherheit verwaltet werden soll. Dies geschieht durch eine Mischung aus Personal, Richtlinien, Abläufen und der Technologie, wobei jeder einzelne Faktor eine entscheidende Rolle bei der Gewährleistung der allgemeinen Sicherheit spielt.

Je mehr Client-Computer es in Ihrem Unternehmen gibt und je aufwändiger Ihre Netzwerkinfrastruktur ist, desto schwieriger wird die IT-Sicherheit. Andererseits beschäftigen die meisten kleinen Unternehmen keine zusätzlichen Mitarbeiter, um die IT-Sicherheitssysteme zu verwalten, sondern übertragen diese Aufgabe leitenden Mitarbeitern.

Falls Sie für die Einrichtung Ihres Sicherheitssystems einen externen Berater hinzuziehen, stellen Sie sicher, dass der Berater durch das bestehende Management Bericht erstattet –

überlassen Sie den Schutz Ihres Unternehmens nicht einem Außenstehenden.

Von einem IT-Sicherheitsberater sollten Sie erwarten, dass er ein *Verzeichnis der Vermögenswerte* aufstellt, also eine Liste aller IT-Vermögenswerte, die sich im Besitz des Unternehmens befinden – von Computern über Router bis zu externen Festplatten. Außerdem müssen die Normen und Maßnahmen vermerkt werden, die das Unternehmen einsetzt, um den Schutz zu maximieren. Das Verzeichnis der Vermögenswerte wird zu einem wichtigen Datensatz und Referenzpunkt, wenn Sie eine IT-Infrastrukturkomponente ändern wollen. Sollte es zu einem Zwischenfall kommen, kann das Verzeichnis der Vermögenswerte Ihnen dabei helfen, die Ursache des Problems zu finden.

Vorausplanung ist beim Einrichten eines Systems zur Informationssicherheit unerlässlich – stellen Sie sich die schlimmsten Szenarien vor und wie Ihr Unternehmen sich davon erholen könnte. Es ist auch wesentlich leichter, sich auf einen Zwischenfall vorzubereiten, bevor er eintritt, als wenn Sie sich mit Ihrem Unternehmen mitten im Zusammenbruch befinden. Dann haben Sie nämlich Schwierigkeiten, auf die benötigten Ressourcen zuzugreifen und die Systeme wiederherzustellen, die die Mitarbeiter für ihre Arbeit brauchen.

Die Funktion der technischen Kontrollen analysieren

Die Technologie spielt sowohl bei den von Ihnen definierten IT-Vermögenswerten als auch bei den eingesetzten Sicherheitssystemen eine wichtige Rolle.

Um den Entwurf wirksamer IT-Sicherheits- und Wiederherstellungssysteme in den Griff zu bekommen, sollten Sie sich Gedanken zu den folgenden Punkten machen:

- Wer trägt die Verantwortung dafür, dass die Systeme immer auf dem neuesten Stand sind und dass Patches übernommen werden, um das System vor Angriffen zu schützen? Wer ist für die Lizenzen der verwendeten Software zuständig?

- Wie wird die Datensicherung verwaltet? Stellen Sie sicher, dass die Aufgaben aufgeteilt sind, so dass nicht die ganze Last an einer Person hängt und die Sicherheit auch dann bestehen bleibt, wenn diese Person krank oder im Urlaub ist.
- Wie kontrollieren Sie den Zugriff auf IT-Ressourcen und Daten? Wie stellen Sie sicher, dass sich die Mitarbeiter beispielsweise beim Surfen im Internet an die Richtlinien halten? Vertrauen Sie ihnen und verlassen Sie sich darauf, dass sie ehrlich sind und die Regeln befolgen? Oder installieren Sie im Rahmen der gesetzlichen Anforderungen passende Filtertechnologien?
- Verfügen Sie über einen Ablauf, der sicherstellt, dass die Gültigkeit vorhandener Sicherheitsrichtlinien nicht durch Änderungen an der IT-Hardware und -Software beeinträchtigt wird?
- Verfügen Sie über einen Wiederherstellungsplan? Welche Maßnahmen haben Sie getroffen, damit Ihr Unternehmen nach schweren Zwischenfällen wie einem Brand oder einem Netzwerkausfall, wiederhergestellt wird?
- Wie ist der Anschluss privater IT-Ressourcen von Mitarbeitern an das Unternehmensnetzwerk und der diesbezügliche Zugriff auf Daten geregelt?

Automatische Lösungen können die Antwort auf einige Fragestellungen dieser Liste sein, sodass sich der Verwaltungsaufwand für die Mitarbeiter verringert. Sie können zum Beispiel den Zugriff mithilfe einer Identitätsverwaltung kontrollieren, die an Mitarbeiter, die sich am Unternehmensnetzwerk anmelden, ein Sicherheits-Token ausgibt. Wahrscheinlich gibt es einen Spam-Filter für Ihre E-Mails, und es ist stark davon auszugehen, dass auch Anti-Malware-Updates bis zu einem gewissen Grad automatisch ausgeführt werden.

Besonders sensible Bereiche Ihrer IT-Architektur können Sie durch Firewalls sperren. In Ihren Plänen zur Stabilisierung der Betriebsabläufe regeln Sie vielleicht die automatische Datensicherung in einen geschützten Online-Speicher. Möglicherweise wollen Sie auch alle Daten, die das Haus verlassen, automatisch verschlüsseln. Sie können auch einen URL- oder Website-Filter installieren, sodass die Mitarbeiter nur auf die Webseiten zugreifen können, die für ihre Arbeit angemessen sind. Das verringert nicht nur das Risiko einer

Sicherheitslücke, sondern erhöht auch die Produktivität der Mitarbeiter – wenn sie nicht auf MySpace zugreifen können, können sie ihre Arbeitszeit auch nicht damit verbringen, ihr Profil zu aktualisieren.

Sicherheitsfunktionen auslagern – die Hosted-Option

Letzten Endes sollte die technische Umsetzung der Sicherheitsrichtlinie nicht Aufgabe des Unternehmens sein. Hier kommt das Hosting ins Spiel: Der IT-Anbieter betreibt die Software (in der Regel webbasiert) für den Kunden. Hosted Security eignet sich nicht für alle Bereiche, funktioniert aber besonders gut in den beiden, mit denen wir uns in den nächsten Abschnitten beschäftigen.

Gehostete E-Mail-Sicherheit

Eine nahe liegende Möglichkeit zur Verringerung des Verwaltungsaufwands ist es, die Spam-Abwehr auszulagern.

Bis zu 95 Prozent aller gesendeten E-Mails sind Spam. Diese zu sortieren kostet Arbeitszeit, Produktivität, Netzwerkbandbreite und Speicherplatz. Spam ist auch eine beliebte Methode zur Verteilung von Malware, sei es durch Phishing-Mails mit Links zu infizierten Websites oder durch fragwürdige Anhänge.

Gehostete E-Mail-Sicherheit filtert diese fragwürdigen E-Mails aus, noch bevor sie das Netzwerk erreichen. Dadurch spart das Unternehmen die Zeit der IT-Mitarbeiter und der Endbenutzer sowie Hardware- und Netzwerkressourcen. Eine Hosted Solution gibt Bandbreite frei und entlastet Ihre Mail-Server, da das Unternehmen von vornherein keinen Spam erhält.

Vorsicht ist jedoch auch hier geboten. Es is ärgerlich, wenn der Spam-Ordner durchsucht werden muss, weil eine E-Mail fälschlicherweise herausgefiltert wurden. Noch schlimmer ist es allerdings, wenn Sie gar nicht erst bemerken, dass Sie diese E-Mail erhalten haben – und es könnte sich ja um etwas Wichtiges handeln, wie zum Beispiel Informationen über ein neues Geschäft. Sie müssen also beim von Ihnen gewählten Anbieter für gehostete E-Mail-Sicherheit auf eine gute (niedrige)

Bilanz hinsichtlich der *Fehlalarme* achten: Wie viele E-Mails werden irrtümlich als Spam markiert? Es kann sogar sein, dass der Anbieter in einem Service Level Agreement eine bestimmte niedrige Anzahl von Fehlalarmen festlegt. Sie können dann also finanzielle Entschädigung fordern, wenn die Anzahl der Falschmeldungen über dem vereinbarte Grenzwert liegt.

Gehostete Endpunkt-Sicherheit

Ein weiterer Bereich, in dem Hosted Security für ein Unternehmen klar von Vorteil sein kann, ist die Verwaltung der Endpunkt-Sicherheit – also der Schutz mehrerer Computer, Laptops, File-Server und anderer Geräte, die Ihre Benutzer eventuell verwenden. Viele dieser Geräte sind bereits mit Sicherheitsprodukten für Privatanwender ausgestattet, denen jedoch die Eigenschaften fehlen, die im geschäftlichen Umfeld verlangt werden. Außerdem müssen sie gesondert verwaltet werden.

Das bedeutet Unterschiede bei den Ablaufterminen, Lizenzen und Konfigurationseinstellungen. Ihr Systemadministrator muss daher mehrere unterschiedliche Produkte beherrschen. Schwerer wiegt jedoch die inkonsistente Sicherheit zwischen den einzelnen Geräten. Es kann auch vorkommen, dass Benutzer die auf ihren Desktops installierten Produkte selbst verwalten, wichtige Updates ausschalten und Ihr Unternehmen dadurch unnötigen Bedrohungen aussetzen. Nehmen die Mitarbeiter dann auch noch ihre eigenen Laptops aus dem Büro mit, entgleitet die Sicherheitsverwaltung völlig Ihren Händen.

Eine gute Lösung zur Vermeidung dieses verwaltungstechnischen Albtraums – insbesondere für kleinere Unternehmen – bietet der Umstieg auf einen Hosting-Anbieter. Dessen Lösungen lassen sich unkompliziert auf mehreren Geräten einrichten. Benutzer müssen nur auf einen Link klicken um die Schutzkomponenten herunterzuladen, die dann innerhalb und außerhalb des Büros funktionieren. Es muss kein Sicherheitsserver betrieben werden, und jeder hat konsistenten, hochwertigen Schutz.

Eine webbasierte, zentrale Management-Konsole bietet einen Überblick über den Zustand jedes einzelnen Gerätes, entdeckte Bedrohungen und vieles mehr.

Kapitel 3

Ein koordiniertes Abwehrsystem aufbauen

In diesem Kapitel geht es um

- Das Entwickeln von Sicherheitssystemen zum Schutz Ihrer IT
- Gedanken zum physischen Schutz
- Aufklärung der Mitarbeiter

Eine starke Sicherheitslösung zeichnet sich nicht durch eine bestimmte Technologie oder Disziplin aus, sondern kombiniert Maßnahmen, die Ihr System vor Angriffen schützen. Einige von Ihnen nutzen Sie wahrscheinlich schon seit Jahren, andere sind Ihnen vielleicht neu. Sie sind aber alle gleich wichtige Details, aus denen sich Ihr gesamter Schutz zusammensetzt.

Vielen Unternehmen fehlen koordinierte Abwehrmaßnahmen gegen Sicherheitsbedrohungen sowie integrierte technische Kontrollen, um die von der Geschäftsleitung entschiedenen Maßnahmen durchzusetzen Es kann sein, dass Sie einige Bereiche hervorragend schützen, zum Beispiel mit einer Firewall: Alles, was auch nur im Entferntesten verdächtig scheint, wird daran gehindert, in das Unternehmensnetzwerk zu gelangen oder es zu verlassen. In anderen Bereichen werden die Benutzer hingegen durch Lösungen für Privatanwender geschützt, wie zum Beispiel durch vorinstallierte Antiviren-Software. Solange aber alle diese Sicherheitselemente nicht aufeinander abgestimmt sind, vermitteln Ihnen diese Insellösungen ein falsches Gefühl der Sicherheit. Wie ist zum Beispiel geregelt, wer die Firewall-Einstellungen überschreiben kann? Und gibt es eine zentrale Management-Konsole für die Sicherheitslösung (die bei einem kleinen Unternehmen vielleicht vom IT-Service-Provider gehostet wird)?

In diesem Kapitel behandeln wir jeden dieser Bereiche etwas genauer. Es geht uns nicht um eine lückenlose Abhandlung, sondern darum, Ihnen einen Überblick zu verschaffen, damit Sie verstehen, wie alle diese Teile zusammenpassen.

Den Zugriff kontrollieren

Zugriffskontrollsysteme stellen sicher, dass die Benutzer, die auf Ihr System zugreifen, wirklich diejenigen sind, die sie vorgeben zu sein. Außerdem müssen sie befugt sein, das zu tun, was sie tun. Darüber hinaus wird sichergestellt, dass sie Ihre Systeme nicht mit Viren oder anderer Malware infizieren und keine Daten entwenden können bzw. keinen unbefugten Zugriff auf Daten erhalten. Zugriffswerkzeuge beinhalten Systeme zur Authentifizierung, zur Identitätsverwaltung, für Rechte, Benutzernamen und Kennwörter.

Ohne Zugriffskontrolle hat ein Hacker leichtes Spiel, in das Netzwerk Ihres Unternehmens einzudringen – aber sofern Ihr Unternehmen nicht mit hochwertigen Gütern handelt, brauchen Sie sich hier auch nicht gleich verrückt machen zu lassen.

Die Netzwerkgrenzen verstärken

IT-Manager und Geschäftsführer verwenden sehr viel Zeit und Mühe darauf, ihre Systeme mithilfe virtueller hoher Zäune zu schützen. Sie kaufen Firewalls und Systeme zur Abwehr von Eindringlingen (IPS, Intrusion Prevention System) oder richten in einigen Fällen VPNs ein (virtuelle private Netze), damit sich die Benutzer auch von außerhalb über eine sichere Verbindung mit dem Unternehmensnetzwerk verbinden können.

Das Verstärken der Netzwerkgrenzen betrifft aber nur die äußerste Abwehrschicht – und keine Netzwerkgrenze ist undurchlässig. Es gibt immer Löcher in diesen Zäunen, wie zum Beispiel den http-Port 80 des Webservers.

Die Identität am Eingangstor überprüfen

Wenn Sie gewaltige Abwehrmaßnahmen einrichten, wie zum Beispiel Firewalls und dergleichen, müssen Sie sich absolut sicher sein, dass Sie keine getarnten Bösewichte hereinlassen.

An dieser Stelle kommt die Zugriffskontrolle ins Spiel – die funktioniert in etwa so, als würden Sie rufen „Wer da?“, bevor Sie die Zugbrücke herunter lassen.

Zugriffskontrolle muss nicht auf komplizierten biometrischen Verfahren basieren, wie zum Beispiel den Ergebnissen eines Iris-Scanners oder Fingerabdrücken, obwohl größere Unternehmen zunehmend diese Methoden nutzen. Allerdings haben die meisten kleinen Unternehmen einen pragmatischeren – und erschwinglicheren – Ansatz zur Identitätsverwaltung.

Heutzutage sind Benutzernamen und Kennwörter die Schlüssel, mit denen man sich Zutritt zum IT-Königreich verschafft. Beides benötigen Sie, um an den Computer zu gelangen, mit dem Sie arbeiten wollen. Mit einem weiteren Kennwort melden Sie sich am Unternehmensnetzwerk an, mit einem anderen an bestimmten Anwendungen, wie zum Beispiel der Buchhaltung, und vielleicht mit noch einem anderen am Bereich mit sensiblen Unternehmensdaten. Das alles versteht man unter dem Begriff Zugriffskontrolle.

Wenn sich jemand von außerhalb am Unternehmensnetzwerk anmeldet, müssen Sie natürlich noch sicherstellen, dass sie oder er nicht den Benutzernamen einer anderen Person missbraucht. Selbst jemand innerhalb des Unternehmens könnte versuchen, etwas ausfindig zu machen, was nicht für sie oder ihn bestimmt ist, wie zum Beispiel das Gehalt und die Zusatzleistungen eines Vorgesetzten.

Die Authentifizierung einer Benutzeridentität basiert in der Regel auf vier Faktoren:

- Was der Benutzer kennt: ein Kennwort oder eine PIN (Persönliche Identifikationsnummer),
- Was der Benutzer hat: eine Chipkarte oder einen Sicherheits-Token,
- Was der Benutzer ist: sein Fingerabdruck oder seine Iris,
- Ein bekannter Ort: innerhalb des Unternehmensgebäudes.

Der Schutz eines Unternehmens wird als ziemlich gut eingestuft, wenn jeder Benutzer zwei dieser vier Tests besteht – schließlich vertraut Ihnen Ihre Bank auch dann, wenn Sie nur mit Karte und PIN Geld abheben. Benötigt Ihr System drei der vier Faktoren, dann ist es wirklich so gut wie uneinnehmbar.

Gute Kennwörter wählen und pflegen

Da es sich bei Benutzernamen und Kennwörtern um die grundlegende Stufe der IT-Sicherheit handelt, ist es wichtig, dass Sie alle Mitarbeiter dazu auffordern, nur schwer zu erratende Kennwörter zu wählen. In der folgenden Liste finden Sie Merkmale für schwer zu erratende Kennwörter:

- Eine Kombination aus Groß- und Kleinbuchstaben und Zahlen.
- Mindestens acht Zeichen Länge.

Außerdem müssen Sie sicherstellen, dass jeder sorgfältig mit seinem Kennwort umgeht. Zu den grundlegenden Punkten für den korrekten Umgang mit Kennwörtern gehören:

- Kennwörter nicht aufschreiben und auch keine diesbezüglichen Notizen in der Nähe des Gerätes, mit dem auf das Netzwerk zugegriffen wird, liegen lassen.
- Keine Standardeinstellungen beibehalten: Die Verwendung des Wortes „Kennwort“ als Kennwort ist einfach zu erraten.
- Keine persönlichen Angaben verwenden, die leicht herauszufinden sind, wie zum Beispiel der Name Ihres ersten Kindes oder Ihres Haustiers.
- Das Kennwort nie an Dritte weitergeben, auch nicht an Kollegen. Nur Ihr IT-Administrator sollte darauf Zugriff haben.

Einschränkende Maßnahmen

Nach der Identifizierung und Authentifizierung kann es sein, dass die Benutzer eine weitere Berechtigungsstufe durchlaufen müssen, damit festgelegt werden kann, welche Aktionen sie durchführen dürfen – ob sie beispielsweise zur Bearbeitung von Dateien oder nur zum Lesen berechtigt sind.

Vielleicht möchten Sie den Zugang in Ihrem Unternehmen so einrichten, dass er auf Rollen basiert, wie das zum Beispiel auch bei der Genehmigung von Ausgaben der Fall ist. Als Leiter der Personalabteilung sind Sie zum Anzeigen und Ändern von Mitarbeiterdaten berechtigt, als Mitarbeiter der Personalabteilung nur zum Anzeigen.

Geht nun der Leiter der Personalabteilung in Urlaub oder wird jemand anderem seine Rolle übertragen, übernimmt diese Person seine Zugriffsrechte auf die Personalakten.

Ihre Telefone und Netzwerke schützen

Es wird viel über Netzwerk- und Gateway-Sicherheit diskutiert. Was einige Unternehmen allerdings nicht mit in Betracht ziehen, ist die Tatsache, dass sie nicht nur ein, sondern viele Netzwerke schützen müssen. Neben dem Internet-fähigen Netzwerk gibt es auch noch das Telefonnetzwerk, ein Intranet und manchmal sogar ein Extranet. Wahrscheinlich gibt es ein WLAN und möglicherweise auch ein VPN oder ein anderes System, mit dem sich Mitarbeiter von außerhalb in das Firmennetzwerk einwählen.

Jedes Netzwerk verfügt wahrscheinlich über ein gewisses Maß an Sicherheit – aber ist es auch das richtige? Es ist die Vernetzung dieser verschiedenen Netzwerke, die das Ganze so kompliziert macht. Wenn zum Beispiel Ihre Internet-Verbindung nicht funktioniert, hätten Sie in der Vergangenheit wahrscheinlich einfach zum Telefon gegriffen und weitergearbeitet. Nutzen Sie aber ein *IP-Telefonsystem (Voice-over-Internet-Protocol)*, mit dem Sie sozusagen über das Internet telefonieren, kann es sehr wohl sein, dass auch das Telefon nicht mehr funktioniert.

Um Telefonnetzwerke herumtelefonieren

Die guten alten Telefonsysteme, insbesondere die Nebenstellenanlagen, waren schon immer das Ziel von Hackern und somit dem Risiko ausgesetzt, abgehört zu werden. Aber nur wenige Kriminelle verfügten über die Technologie und das Fachwissen, um solche Angriffe zu organisieren.

Heutzutage allerdings schalten viele Unternehmen ihre Telefonnetzwerke auf IP-Telefonie (VoIP) um, da sie dadurch eine deutlich niedrigere Telefonrechnung haben und das gleiche Netzwerk wie für ihre Daten nutzen können. Und das wiederum bedeutet weniger Infrastrukturkosten und weniger Verwaltung.

Illegal in ein VoIP-System einzudringen oder es zum Erliegen zu bringen ist einfacher, da es im selben Netzwerk wie das Computer-System ausgeführt wird. VoIP-Systeme sind also angreifbar für:

- **Betrug:** Ein Cyberkrimineller dringt illegal in Ihr VoIP-System ein, tätigt etliche Anrufe zu teuren, kostenpflichtigen Nummern, und Sie müssen am Ende die Rechnung bezahlen.
- **Denial-of-Service-Angriffe (DoS):** Genauso wie bei den DoS-Angriffen auf Websites versucht ein Cyberkrimineller Ihren Telefondienst zum Erliegen zu bringen und so seine Nutzung zu verhindern.
- **Spam- und Phishing-Angriffe:** Wie bei einem Computer-System rufen hier Computer mit Sprachausgabe ununterbrochen verschiedene Nummern an. Ziel ist es, jemanden zu einem betrügerischen Kauf oder sinnloser Zeitverschwendung zu verleiten.

Die Tatsache, dass Sie es mit Internet-Protokollen zu tun haben, bedeutet, dass Sie den gleichen Schutz verwenden sollten wie für Ihre Computer-Systeme. Bedenken Sie jedoch, welches Risiko mit dem Ausfall der Telefonleitung verbunden ist. Vielleicht ist es besser, Ihr VoIP-System von den Computer-Systemen zu isolieren.

Drahtlose Netzwerke schützen

Bei der ersten Generation drahtloser Verbindungen waren die Benutzer zu nachlässig, um die Sicherheitsfunktion an Routern und Zugangspunkten zu aktivieren: einerseits, weil es ein komplizierter Vorgang zu sein schien, andererseits aber auch, weil man sich der Risiken nicht bewusst war.

Sie müssen wissen, dass heutige drahtlose Verbindungen spezielle Sicherheitsrisiken bergen, die sich in vier Kategorien aufteilen:

- **Trittbrettfahrer:** Andere Benutzer verbinden sich über Ihren Zugang mit dem Internet, haben dadurch vollständigen Zugriff auf das Netzwerk und seine Ressourcen und beeinträchtigen die Leistungsfähigkeit Ihres Systems. Zu dieser Situation kommt es, wenn keine Authentifizierung oder Verschlüsselung aktiviert ist.
- **MAC Spoofing:** Hacker finden die MAC-Adresse (Media Access Control) Ihres Netzwerks heraus und nutzen sie, um sich Zugriff zu verschaffen und den Netzwerkverkehr zu stören.
- **Denial-of-Service-Angriff:** Ein Cyberkrimineller hindert befugte Nutzer, auf das drahtlose Netzwerk zuzugreifen.
- **Man-in-the-Middle-Angriff:** Ein Hacker richtet einen falschen Zugangspunkt ein, über den er Ihren gesamten Netzwerkverkehr abhören und falsche, aber seriös erscheinende Nachrichten einschleusen kann.

Ein älterer Standard der drahtlosen Sicherheit wurde jetzt durch die WPA- und WPA2-Verschlüsselung ersetzt. Solange Sie Ihr WLAN mit einem sicheren Kennwort installieren und sich dieses Kennwort gut merken, sollten Ihre Netzwerkverbindungen ziemlich sicher sein. Die WPA- sowie die WPA2-Verschlüsselung authentifiziert Benutzer, um zu überprüfen, ob sie zugriffsberechtigt sind, und verschlüsselt die Daten, die zwischen Benutzer und Netzwerk übertragen werden.

Es kommt sogar noch besser: Die Gerätehersteller haben dieses Sicherheitsprotokoll nämlich so konzipiert, dass es ganz einfach einzurichten ist. So können Sie Ihr drahtloses Netzwerk in nur wenigen einfachen Schritten absichern.

Computernetze schützen

Die Computernetze kleiner Unternehmen waren schon immer angreifbar – und die Sicherheitsmaßnahmen in der Regel recht wirksam. Schätzungen zufolge haben 80 bis 90 Prozent aller Unternehmen in Firewalls investiert und 50 bis 60 Prozent in IPS-/IDS-Systeme (Erkennung und Abwehr von Eindringlingen). Die Integration dieser Technologie in Geräte mit einem Microsoft Betriebssystem hat diese Zahlen sogar noch erhöht.

Eine *Firewall* verhindert den unbefugten Zugriff auf das Netzwerk, während ein *Intrusion Detection/Prevention System* die Netzwerkaktivität überwacht und nach bösartigem oder anormalen Verhalten sucht, darauf reagiert und es stoppt.

Das Problem mit Technologien für die Computersicherheit ist, dass Sie Ihr Unternehmen so vollständig abschotten, dass kein normaler Geschäftsbetrieb mehr möglich ist, da Sie jeden Alarm für einen Angriff halten. Gehen Sie zu weit in die andere Richtung, macht es fast keinen Sinn mehr, diese Technologie einzusetzen. Der Trick ist also größtenteils, sich mit den Fähigkeiten der Technologie vertraut zu machen. Außerdem sind die Technologiehersteller dabei, den Netzwerkadministratoren vieles leichter zu machen.

Netzwerk-Firewalls und IPS/IDS werden immer öfter zusammen mit anderer Funktionalität auf einem UTM-Gerät (Unified Threat Management, vereintes Bedrohungsmanagement) integriert. Dabei handelt es sich in der Regel um kleine, eigenständige Hardware, die das kleine Unternehmen buchstäblich nur noch kaufen und installieren muss und dann vergessen kann.

Ein Unternehmen mit externen Benutzern, die sich mit dem Firmennetzwerk verbinden wollen, oder eine Firma, die Zweigstellen mit dem Hauptnetzwerk verbinden will, kann ein *virtuelles privates Netzwerk (VPN)* einrichten, das mit unterschiedlichen Methoden eine gesicherte Verbindung aufbaut. Da das VPN eine Vielzahl von Sicherheitsprotokollen verwendet – in der Regel Internet Protocol Security (IPSEC) für standortübergreifenden Zugriff und Secure Sockets Layer (SSL) für den Zugriff externer Benutzer – ist es meist sehr sicher. Es „tunnelt“ nämlich die gesamte Kommunikation mit dem Netzwerk und verschlüsselt dabei die Daten.

Überlegen Sie sich genau, wie Sie die Benutzer anbinden und wie Sie die Benutzer eines VPNs authentifizieren. Was passiert zum Beispiel, wenn ein Benutzer seinen Laptop im Zug liegen lässt? Könnte ein Fremder den Computer an sich nehmen und auf Ihr Firmennetzwerk zugreifen?

Die Oberhand über die Sicherheitsverwaltung behalten

Vieles, was die IT-Sicherheit ausmacht, gehört zu den grundlegenden Tätigkeiten der IT-Administration. Stellen Sie daher sicher, dass Sie die wichtigsten organisatorischen Aufgaben, die für Ihre geschäftliche IT-Infrastruktur erforderlich sind, durchführen. So muss beispielsweise gewährleistet sein, dass die Software auf dem neuesten Stand ist und Patches übernommen werden – ein wichtiger Bereich, da immer mehr Fehler in einer Vielzahl von Systemen und Software entdeckt werden. Zugleich kann es die Aufgabe der Sicherheitsverwaltung sein zu überprüfen, ob die Benutzer die neueste Version der Sicherheitsupdates erhalten.

Zero-Day-Angriffe vermeiden

Zero-Day-Sicherheitsangriffe, die Schwachstellen in Softwaresystemen ausnutzen, noch bevor der Anbieter einen Patch verteilen kann, nehmen zu. Dabei sind vor allem Webbrowser zu einer bevorzugten Zielscheibe geworden. Der Grund: Sie decken eine große Benutzerzahl ab und können unmittelbar ausgenutzt werden, sobald ein Benutzer auf einer infizierten Webseite ist. Der Ansatz von Microsoft, einmal monatlich am „Patch-Dienstag“ Updates herauszugeben, gibt den Cyberkriminellen einen ganzen Monat Zeit zur Nutzung einer Schwachstelle, bevor eine Nachbesserung veröffentlicht wird.

Außer einer guten Organisation kann ein Geschäftsführer nicht viel tun, um sein Unternehmen vor Zero-Day-Angriffen zu schützen. Allerdings hilft es, durch proaktives Verhalten einen Überblick über die größten Schwachstellen und Bedrohungen zu behalten und vorläufige Maßnahmen zu treffen, um so Probleme notdürftig beheben zu können.

Ein Großteil der Sicherheitsverwaltung kann heute automatisiert werden, einschließlich der Nachbesserung durch das *Windows Update,* dem automatischen Service von Microsoft. Dieser stellt sicher, dass die Microsoft Software immer auf dem neuesten Stand ist und aktualisiert automatisch Viren- und Spyware-Datenbanken. Sie können sogar einige der in Ihrer Sicherheitsrichtlinie enthaltenen Regeln durchsetzen, indem Sie zum Beispiel den Zugriff auf bestimmte Anwendungen für bestimmte Arten von Benutzern sperren.

Den Benutzerzugriff einschränken

Sie können solche Einschränkungen auch in Ihre Internet-Nutzungsrichtlinie mit aufnehmen. Zum Beispiel, dass es zwischen 9 und 13 Uhr sowie 14 und 18 Uhr nicht gestattet ist, auf die Websites sozialer Netzwerke zuzugreifen. Ein Beispiel für allgemeine Nutzungsbedingungen finden Sie in Kapitel 2. Aber wie setzen Sie diese Bedingungen durch? Sie können nicht auf Patrouille durch das Büro gehen und überprüfen, was sich die Mitarbeiter so auf ihren Desktops anschauen. Ein URL-Filter kann hier mit seiner hohen Flexibilität und einer Website-Kategorisierung den Zugriff auf anstößige Inhalte gemäß der von Ihnen erstellten Richtlinie sperren und dadurch möglicherweise Stunden an verlorener Produktivität sparen.

Die Sicherheitsrichtlinie enthält auch Angaben zu Funktionen und Verantwortungsbereichen – eine Art Organisationsdienstplan. In einem kleinen Unternehmen kommt es aber eher selten vor, dass dies die Hauptaufgabe eines Mitarbeiters ist. Daher ist es wichtig sicherzustellen, dass diese Aufgabe wie festgelegt durchgeführt wird.

Die Technik betreuen

Zur Sicherheitsverwaltung gehört auch die Betreuung der Anti-Malware- (Virenschutz und Anti-Spyware) und Anti-Spam-Technologie. Die Anti-Malware-Technologie wird von großen wie kleinen Unternehmen gleichermaßen stark genutzt, nämlich von über 95 Prozent. Es handelt sich hier auch um eine voll ausgereifte Technologie, bei der sich die führenden Produkte nur wenig unterscheiden.

Die besten heutzutage verwendeten Anti-Malware-Schutzfunktionen haben folgende Eigenschaften:

- Externe Datenbanken für Sicherheitsupdates, um Systeme des Unternehmens zu entlasten, plus gehostete Lösungen für E-Mail- und Endpunkt-Sicherheit. Mehr dazu in Kapitel 5.
- Automatischer Abgleich möglicher Bedrohungen mit Bedrohungen in den externen Datenbanken durch den Computer.
- Zentrale Verteilung von Systemen und Upgrades, ohne diese vor Ort auf jedem Desktop selber einspielen zu müssen.
- Zentrale Verwaltung und Berichterstattung.
- Verbesserte Kompatibilität mit älteren Betriebssystemen und Hardware-Geräten.
- Automatische Entfernung/Quarantäne von Malware und schnelle Berichterstattung/Überwachung für die Systemadministratoren.

Viele Malware-Infektionen werden dadurch verursacht, dass der Benutzer wissentlich oder unwissentlich Software herunterlädt. Er wird zum Beispiel zum Download eines vermeintlichen Updates für eine bestimmte Anwendung verleitet und muss dann feststellen, dass die Update-Benachrichtigung eine Fälschung war und er sich in Wirklichkeit einen Wurm oder einen anderen Virus heruntergeladen hat.

Systemadministratoren würden die Desktop-Umgebung am liebsten so absichern, dass die Benutzer nur minimale Änderungen an der Konfiguration vornehmen können und alle diese Änderungen am Ende einer Sitzung wieder gelöscht werden. Dieser *unberührte Zustand* vereinfacht es den Administratoren, einen Überblick über die Software zu behalten und minimiert, zumindest theoretisch, die meisten Infektionsquellen.

Derart abgesicherte Desktop-Umgebungen sind für öffentliche Bereiche oder Geräte geeignet, die von wechselnden Benutzern verwendet werden. Dazu gehören Hotdesk-Umgebungen (wo Mitarbeiter an mehreren Arbeitsstationen tätig sind)

und vielleicht sogar mobile Anwender. Ob sie allerdings das Richtige für das gesamte Unternehmen sind, ist eine andere Frage.

Unternehmen sollten das Ausleihen von Laptops durch Mitarbeiter in einer entsprechenden Richtlinie festlegen. Das Absichern der Desktop-Umgebung kann hier bei der Durchzusetzung helfen. Allerdings müssen Sie berücksichtigen, ob Sie dadurch nicht die Produktivität Ihrer Mitarbeiter beeinträchtigen.

Datensicherheit gewährleisten

Bei der Datensicherheit geht es um den kontrollierten Zugriff auf Daten und deren Schutz vor Missbrauch. Das Thema sorgt immer wieder für Schlagzeilen, wenn Politiker und Staatsangestellte ihren Laptop im Zug oder Flugzeug vergessen und persönliche Daten dadurch jedermann zugänglich machen.

Jenseits der Schlagzeilen geht es den Unternehmen aber ganz einfach um den Schutz vertraulicher Kundendaten und um ihre juristische Verantwortung, die persönlichen Daten ihrer Mitarbeiter vor unbefugtem Zugriff zu schützen.

Die Reichweite von Datenbanken erkennen

Aufgrund der Vernetzung heutiger Systeme können Sie nicht davon ausgehen, dass Daten in einem eigenständigen System sicher sind – die Datenbank selbst muss geschützt werden, genauso wie alle Anwendungen, die auf sie zugreifen.

Cyberkriminelle waren und sind sehr erfolgreich darin, Datenbanken auszubeuten, wenn die zugehörige Webanwendung mit veraltetem Code und veralteten Werkzeugen arbeitet. Stellen Sie sich vor, Sie haben eine Datenbank und die Webanwendung, die mit dieser Datenbank kommuniziert, hat eine Schwachstelle. Dann kann jeder, der die Schwachstelle ausnutzt, eine entsprechende Anfrage stellen, Zugriff auf die Datenbank erhalten und theoretisch alle dort gespeicherten Daten einsehen.

Man hört nicht oft von dieser Art von Gefahr, da niemand ein Interesse daran hat, es zuzugeben. Doch für das Unternehmen kann dies katastrophale Folgen haben und die Geschäftsleitung harter Kritik aussetzen.

E-Mail-Bedrohungen eindämmen

E-Mails bergen ein ungeheures Potenzial für den Verlust von Daten, da sie in der Regel nur durch Benutzername und Kennwort geschützt sind. Aber es ist beruhigend zu wissen, dass die Suche nach einer E-Mail mit sensiblen Daten aufgrund der großen Menge an Nachrichten der Suche nach einer Nadel im Heuhaufen ähnelt.

Eine E-Mail ist von Natur aus ein unsicheres Medium, und für E-Mails mit sensiblen Geschäftsdaten ist Verschlüsselung immer noch die bessere Lösung. Bei der *E-Mail-Verschlüsselung* werden Schlüssel sowohl für die Authentifizierung des Benutzers als auch für den Schutz sensibler Daten verwendet.

Die Wahrnehmung des Datenschutzes in Hinblick auf Mitarbeiter-E-Mails am Arbeitsplatz wird viel diskutiert. Sind E-Mails das persönliche Eigentum des Empfängers oder des Unternehmens? Allerdings sollte eine vernünftige E-Mail-Richtlinie das Unternehmen vor den meisten derartigen Problemen schützen. Kapitel 2 erörtert allgemeine Nutzungsbedingungen.

Sorgfältig mit Daten umgehen

Oft gehen Daten verloren, wenn Informationen in einem Unternehmen weitergeleitet werden – auf einem USB-Stick zum Beispiel, oder wenn jemand einen Teil einer Datei zum Analysieren ausschneidet und es dann nicht mehr vom Laptop entfernt.

Datenlecks entstehen eher dann, wenn Daten übertragen werden – oder wenn Mitarbeiter sich nicht an die vom Unternehmen festgelegten Richtlinien halten.

Auch hier kann Automatisierung hilfreich sein, indem zum Beispiel Daten automatisch verschlüsselt werden, sobald sie auf einen USB-Stick übertragen werden. Alternativ kann

zum Beispiel auch eine Lösung angewendet werden, die gewährleistet, dass Daten auf einem Laptop automatisch verschlüsselt werden.

Physische Sicherheit bereitstellen

Die Sicherung des Firmengeländes, der Einrichtung, der Mitarbeiter, der Computersysteme und anderer Vermögenswerte erfordert wahrscheinlich die meiste Arbeit bei der Sicherheitsverwaltung. Wenn Sie jetzt vielleicht denken, dass physische Sicherheit in einem Buch über IT-Sicherheit nichts zu suchen hat, dann liegen Sie falsch.

Physische Sicherheit stellt die erste Verteidigungslinie für IT-Systeme dar und ist eine wesentliche Voraussetzung dafür – der einfachste Weg für einen Cyberkriminellen, Daten zu stehlen oder Systemen zu schaden, besteht darin, physischen Zugriff auf die Daten bzw. das System zu gewinnen.

Für den Schutz Ihres Firmengeländes haben Sie wahrscheinlich schon gesorgt, und die Risiken für die IT-Vermögenswerte werden an Ihren Maßnahmen nichts ändern. Allerdings kann es sein, dass Sie sich nach einer Überprüfung der IT-Vermögenswerte in Ihrem Unternehmen entscheiden, in einigen Bereichen zusätzliche Schutzmaßnahmen anzubringen. Nicht nur aufgrund des Gerätewerts, sondern auch wegen der dort gespeicherten Daten und wegen der Störung, die bei einem Systemausfall für den Geschäftsbetrieb entstehen würde.

So ist zum Beispiel ein gesicherter Zugang zum Serverraum, wenn Sie denn einen haben, ein wesentlicher Punkt. Jeder, der diesen Raum betritt oder verlässt, sollte durchleuchtet werden, denn nur so können Sie sicherstellen, dass er oder sie nicht ein mobiles Medium bei sich trägt, auf das Daten kopiert werden können.

Schlösser, Safes, Alarmsysteme und Sicherheitsbeamte sind bewährte Sicherheitsmethoden, und modernere elektronische Geräte können ebenfalls helfen:

- Videoüberwachungskameras an bestimmten Zugangspunkten, die mit einem Computernetzwerken verbunden werden können, damit unabhängig vom Standort Aufzeichnungen gemacht und abgespielt werden können.
- Monitore, Kabel und Controller werden immer erschwinglicher für kleine Unternehmen.
- Alarmsysteme, nicht nur rund um ein Gebäude, sondern in besonders strategisch günstigen Positionen, werden ebenfalls immer günstiger und lassen sich vielfach selbst installieren.
- Zugangskontrollsysteme, wie z. B. Karten, PIN-Nummern und Sprechanlagen, wurden in der Vergangenheit nur von größeren Unternehmen genutzt, sind aber jetzt für alle unverzichtbar.

Für danach planen

Keine Sicherheitsrichtlinie kommt ohne Plan zur Stabilisierung des Betriebsablaufs und zur Wiederherstellung aus. Zu planen, wie man auch angesichts einer Katastrophe geschäftsfähig bleibt, hat für jedes Unternehmen höchste Priorität. Dabei ist es egal, ob es sich um eine technische Störung, den Ausfall der Website oder eine Naturkatastrophe handelt, wie z. B. einen Brand auf dem Firmengelände. Die *Stabilisierung des Betriebsablaufs* konzentriert sich darauf, eine Unterbrechung der Geschäftstätigkeit auch angesichts einer solchen Katastrophe zu vermeiden, während die *Wiederherstellung* sich damit beschäftigt, die IT-Systeme nach einem solchen Zwischenfall wieder in den ursprünglichen Zustand zu versetzen..

Bei Planungen zur Stabilisierung der Business Continuity wird oftmals von Worst-Case-Szenarien ausgegangen, für die dann Wiederherstellungsmaßnahmen entwickelt werden müssen. Da es aber relativ unwahrscheinlich ist, dass Ihr Unternehmen mit einer Naturkatastrophe oder einem Terrorangriff konfrontiert wird, ist es besser, sich den Plan für den Erhalt der Business Continuity wie einen Schutzschild für alle tagtäglichen Szenarien vorzustellen. Dazu gehören zum Beispiel Stromausfälle, der Konkurs eines Lieferanten, Überschwemmungen oder Stürme.

Wenn Sie sich die Frage stellen, ob der Erhalt der Business Continuity wirklich wichtig ist, sollten Sie sich vor Augen halten, dass die meisten kleinen Unternehmen ein Worst-Case-Szenario nicht überstehen:

- Von den 350 Unternehmen, die 1993 von den Angriffen auf das World Trade Centre in New York betroffen waren, gingen 150 bankrott. Bei denen jedoch, die fortbestanden – und darunter gibt es einige bemerkenswerte Beispiele – lief der Geschäftsbetrieb bereits wenige Tage nach der Katastrophe wieder stabil.
- Der Brand im Öldepot Buncefield 2005 in der Nähe von London – der größte Brand in Europa seit dem Zweiten Weltkrieg – sorgte für beträchtliche Störungen im Betriebsablauf. Das Büro von Northgate Information Solutions in Hemel Hempstead, direkt neben dem Depot, wurde komplett zerstört. Einige Websites von Unternehmen des öffentlichen Dienstes, die die Firma hostet, waren zeitweise außer Betrieb. Aber Northgates Pläne zur Stabilisierung des Betriebsablaufs gewährleisteten, dass die Kunden nicht zu viel Schaden erlitten, und am Monatsende hatte das Unternehmen alle seine internen Systeme und die überwiegende Mehrheit der Daten wiederhergestellt.

Hackerangriffe und die Manipulation von Daten erscheinen im Vergleich dazu ziemlich unbedeutend. Aufgrund der Störung, die sie bei der Geschäftskontinuität verursachen, finden sie sich dennoch in der Liste der schwerwiegendsten Bedrohungen.

Zu den allgemein üblichen Bedrohungen stabiler Betriebsabläufe gehören:

- Naturkatastrophen (Überschwemmungen, Erdbeben, Brände usw.)
- Cyberangriffe
- Interne Sabotage
- Stromausfall
- Terrorismus
- Krankheiten (wie zum Beispiel eine Grippepandemie)
- Festplattenausfall.

Nachdem Sie die Bedrohungen identifiziert, ihre negativen Auswirkungen analysiert und Pläne zur Stabilisierung der Business Continuity erstellt haben, müssen Sie jetzt das Testen und Warten Ihrer Systeme gewährleisten. Viele Unternehmen hören mit der Formulierung des Plans auf, in der Annahme, dass sie jetzt geschützt seien. Dies ist aber nicht der Fall. Tests und Wartung der Pläne ist entscheidend für ihre Wirksamkeit im Katastrophenfall.

Im Ernstfall funktionieren Pläne zur Wiederherstellung nach schwerwiegenden Ereignissen (Desaster Recovery) am effektivsten. Pläne zur Behebung eines Systemausfall, eines Angriffs auf Websites oder einer Malware-Infektion sind hingegen meist weniger effektiv. Das liegt wahrscheinlich daran, dass sie weniger strikt strukturiert sind und nicht so rigorose Abläufe definieren.

Machen Sie Ihre Benutzer auf Ihre Pläne aufmerksam

Ein entscheidender Schritt für die Wirksamkeit Ihrer Pläne ist, dass Ihre Mitarbeiter über die Existenz der Pläne, der Personalrichtlinien und -maßnahmen sowie der Verhaltensregeln der IT-Sicherheit Bescheid wissen.

Viele kleine Unternehmen teilen den Mitarbeitern nicht mit, was sie unter „zulässiger Nutzung“ verstehen oder was ein schwer zu erratendes Kennwort ausmacht. Während die Betriebsleitung also davon ausgeht, dass die bewährten Methoden befolgt werden, wissen die Mitarbeiter nicht einmal, dass es diese bewährten Methoden gibt. Wenn Sie Ihren Mitarbeitern die Pläne und Richtlinien nicht mitteilen, wie sollen sie sich dann daran halten können?

Nur wenige Menschen wollen einem Unternehmen absichtlich schaden oder es unnötigen Risiken aussetzen, aber es kann sein, dass Mitarbeiter Ihr Unternehmen durch Unkenntnis über die Richtlinien in Gefahr bringen. So kann das scheinbar harmlose Surfen im Internet oder eine Datenübertragung zu alarmierenden Ausfällen führen, die Cyberkriminelle anschließend ausnutzen. Während Sie zwar Einzelpersonen beauftragen, die Sicherheit Ihres Unternehmens zu

überwachen und zu lenken, liegt diese Verantwortung letztendlich bei jedem einzelnen Mitarbeiter.

Menschen sind oft das schwächste Glied in der IT-Sicherheit. Aufklärung und fortlaufende Sensibilisierung sind das I-Tüpfelchen bzw. das Puzzleteil, das nur allzu oft fehlt – mit anderen Worten, die letzte Hürde im Rennen um die perfekt funktionierende IT-Sicherheit.

Cyberkriminalität ist nämlich meist so konzipiert, dass sie die Benutzer zu einer Aktion verleitet, die dann ihrem Unternehmen schadet. Dabei handelt es sich meist um eine Aktion, die die Benutzer nicht durchgeführt hätten, wenn sie vorher darüber nachgedacht hätten. Dazu gehören:

- Das Klicken auf einen Link in einer Spam-Mail
- Der Besuch auf einer Website mit anstößigen Inhalten
- Die Übergabe persönlicher oder unternehmensinterner Daten an einen unbekannten Dritten
- Das Mitnehmen vertraulicher Daten aus dem Unternehmen
- Das Übergehen von Sicherheitsupdates oder Backups um Zeit zu sparen.

Die Publikation von Sicherheits – und Mitarbeiterrichtlinien, ergänzt durch Aufklärung über ihre Wichtigkeit, gewährleistet zumindest eine grobe Einhaltung der Regeln. In Trainings sollte immer wieder auf den Grundsatz des geringsten Vertrauens hingewiesen werden: Wenn Sie nicht sicher sind, dass der E-Mail-Anhang in Ordnung ist, öffnen Sie ihn nicht.

Kontinuierliche Sensibilisierung und Trainings sind aber auch wichtig, um den Cyberkriminellen immer einen Schritt voraus zu sein.Das gilt insbesonders, da sich Richtlinien ändern können, aber auch, um den Mitarbeitern gegenüber das beständige Engagement der Geschäftsleitung für einen starken Schutz deutlich zu machen. Cyberkriminelle suchen nach immer neuen Wegen, um die Benutzer zu Dingen zu verleiten, die sie eigentlich nicht tun sollten. Daher ist es wichtig zu gewährleisten, dass jeder stets auf der Hut ist – und wenn etwas verdächtig aussieht, dann ist es das wahrscheinlich auch.

Kapitel 4

Kenne deinen Feind

In diesem Kapitel

- Erhalten Sie einen Überblick darüber, wie sich Bedrohungen entwickelt haben
- Lernen Sie die gravierendsten Bedrohungen, mit denen Ihr Unternehmen konfrontiert ist, kennen und verstehen
- Erfahren Sie etwas über die junge Geschichte der Cyberangriffe
- Erkunden Sie die Unterwelt der Cyberkriminellen

Die Bedrohungslandschaft hat sich in den letzten zehn Jahren dramatisch verändert: Von den massenhaften Ausbrüchen, die zu Beginn des Jahrzehnts Schlagzeilen machten, bis zu den heimlicheren, untereinander vernetzten Internet-Bedrohungen von heute. Auch bei der Anzahl der Bedrohungen ist ein enormer Anstieg zu verzeichnen. So stellt z. B. der Virenforscher AV-Test monatlich 700.000 neue Malware-Instanzen fest. Die Menge allein macht es schon schwieriger, Bedrohungen zurückzuverfolgen und sie zu bekämpfen, aber auch die Cyberkriminellen im Untergrund sind heute andere als früher. Während es damals nach Ruhm strebende Amateure waren, ist es jetzt eine profitorientierte Schattenwirtschaft.

Kleinere Unternehmen sind anfälliger für gezielte Angriffe, da sie oft nicht über die IT-Ressourcen zur Abwehr verfügen und nicht entsprechend reagieren können.

Die beste Strategie zur Verteidigung gegen diese sich entwickelnden Bedrohungen ist es, seinen Gegner zu kennen. Das folgende Kapitel untersucht die Bedrohungen von heute und die Kriminellen, die dahinter stehen, nun etwas genauer.

Nur der Gerissenste gewinnt – Die junge Geschichte der Cyber-Bedrohungen

Vor Beginn des 21. Jahrhunderts und in den ersten Jahren danach waren massenhafte Viren-, Würmer- und Trojaner-Ausbrüche die häufigste Form von Malware. Der 1999 erstmalig entdeckte Melissa-Virus versuchte bekanntermaßen, sich an die ersten 50 Einträge im E-Mail-Adressbuch eines Benutzers zu versenden. Auch der ILOVEYOU-Virus, der im darauf folgenden Mai in Erscheinung trat und zur Bedrohung mit dem bis dahin größten finanziellen Schaden wurde, versendete sich an alle E-Mail-Adresseinträge eines Benutzers – zusammen mit einem „Liebesbrief" im Anhang, der beim Öffnen erheblichen Schaden verursachte. 2001 folgte dann „Code Red", 2003 waren es „SQL Slammer" und „Sasser".

In den folgenden Jahren entstanden weitere zahlreiche Wurm- und Virenvarianten, die zumeist Schwachstellen in Microsoft Systemen ausnutzten (wegen deren weiter Verbreitung). Mit der Zeit nahm die Schlagkraft ihrer Schadteile jedoch ab: Einerseits wurden sie in großer Zahl durch immer wirksamere Antiviren-Software abgefangen, andererseits wurden die Benutzer immer umsichtiger.

Die Anfänge der Spam-Epidemie

Zwischen 2001 und 2003 begannen die Cyberterroristen, Massen-Mails zu versenden. Mithilfe von *Phishing-Techniken*, also dem Versenden seriös aussehender E-Mails, wollten sie nichts ahnende Benutzer dazu verleiten, ihre Bankverbindungen und andere persönliche Angaben preiszugeben.

2004 nahm das Spam-Problem epidemische Ausmaße an, so dass 70 bis 80 Prozent aller E-Mails, die bei Unternehmen eingingen, als Spam eingeordnet werden konnten. Ungefähr zur selben Zeit begannen die Virenschreiber auch, ihren Schadteil an E-Mail-Nachrichten anzuhängen.

Auch diese Spam-Flut konnte durch technisch ausgereiftere Spam-Filter etwas eingedämmt werden. E-Mails werden jetzt nicht nur wegen verdächtig erscheinender Betreffzeilen oder Absender als Müll eingeordnet, sondern auch aufgrund ihres Inhalts. Eine Weiterentwicklung sind gehostete Anti-Spam-Technologien: Sie gewährleisten, dass Spam und andere E-Mail-Bedrohungen gestoppt werden, bevor sie das Netzwerk erreichen, um so zu verhindern, dass die Masse

(Fortsetzung)

(Fortsetzung)

an unerwünschten E-Mails die Mail-Server und Netzwerke weiter überlastet.

Beobachtende Spyware

Seit 2004 gehört *Spyware* (unwissentlich heruntergeladene Software, die die Computeraktivität des Benutzers aufzeichnet) zum Arsenal der Cyberkriminellen. Diese Bedrohung ist weitaus schlimmer und schwerer verfolgbar. 2004 hatten, nach einer Studie von AOL und der National Cyber-Security Alliance, 80 Prozent aller Privatanwender die eine oder andere Spyware auf ihrem Computer, ohne dass sie sich dessen bewusst waren.

Die Entwicklung von Spyware war umso Besorgnis erregender, als sich die Antiviren-Anbieter zum Zeitpunkt ihres Auftretens noch in eine ganz andere Richtung orientierten. Herkömmliche Antiviren-Produkte konnten keine Spyware entdecken, da sie im Vergleich zu Viren vollkommen andere Eigenschaften aufweist. Mittlerweile enthält fast jede Rundum-Sicherheitssuite eine Anti-Spyware-Komponente und die meisten Unternehmen werden jetzt geschützt.

Bot-Netz-Kriege

Auf Spyware folgten die Bots, kurz für Robot (Roboter). Bots sind infizierte Computer, die ein *Bot-Netz* bilden, wenn mehrere von ihnen zusammengeschlossen werden. Sie tun, was ihnen ihr Bot-Master befiehlt, nämlich Angriffe zu starten: von DoS bis hin zum Versenden von Massen-Spam-Mails.

Die Rechenleistung eines Bot-Netzes übersteigt die eines herkömmlichen Cyberangriffes um das Hundertausendfache. Ihre konzentrierten, gezielten Aktionen können ernsthafte Schäden verursachen. Einige Fachleute glauben, dass moderne verteilte Computertechniken zur Verbreitung der Bot-Netze beigetragen haben, da in kurzer Zeit eine Vielzahl von Computern durch Dateifreigaben und Peer-to-Peer-Netzwerke infiziert werden kann..

Schutz vor den komplexen Internet-Bedrohungen von heute

Wenn man aus der Entwicklung von Bedrohungen in den letzten zehn Jahren irgendetwas lernen kann (siehe „Nur der Gerissenste gewinnt – Die junge Geschichte der Cyberbedrohungen“ in der Seitenleiste), so ist es dies: Sobald Sie ein Loch in Ihren Abwehrsystemen stopfen, müssen Sie sich um das nächste kümmern. Heutzutage sind die Grenzen

zwischen den verschiedenen Arten von Malware fließend, und was in der Vergangenheit noch ein relativ einfacher, linearer Angriff war, hat sich zu einem komplexen, oft sogar dauerhaften Angriff gewandelt.

In der Vergangenheit wurde die Bedrohung (und oft auch die damit verbundene Abwehr) durch die Angriffsmethode definiert, doch die Cyber-Kriminellen werden immer raffinierter. Sie bauen auf den wirksamsten Schadteilen der vorherigen Generation auf, integrieren zugleich neue Angriffsmethoden und verändern ständig ihre Angriffspunkte, um einer Entdeckung zu entgehen. Ihre neuen Angriffe vereinen eine Reihe schädlicher Eigenschaften mit möglicherweise desaströser Wirkung.

Diese komplexen Bedrohungen werden als *Internet-Bedrohungen* bezeichnet, da sie zum größten Teil webbasiert sind. Laut einer 2008 von TrendLabs (dem Sicherheitslabor von Trend Micro) durchgeführten Studie, die zahlreiche Computerinfektionen bis an ihre Ursprünge zurückverfolgte, erreichen über 90 Prozent der Bedrohungen ihr Angriffsziel über das Internet. An zweiter Stelle lag die Dateiübertragung, wobei Wechselmedien wie USB-Laufwerke verwendet wurden.

Das Internet ist der perfekte Ort, um einen Cyberangriff zu starten. Es liefert ein Massenpublikum möglicher Opfer, und die Cyberkriminellen können ihre wahre Identität bis zu einem gewissen Grad vor dem Benutzer verbergen. Natürlich sind auch Cyberangriffe einfach zurückzuverfolgen, da sie von einer bestimmten Internetadresse kommen, die gesperrt werden kann. Allerdings werden die Kriminellen dadurch nur dazu gezwungen, sich ihrem nächsten Opfer zuzuwenden.

Ein Blick auf tödliche Kombinationen

Komplexe Internet-Bedrohungen sind oft mehrstufig. Was anfangs harmlos erscheint, wie zum Beispiel eine E-Mail mit einem Link, kann beim Öffnen einen Schadteil auslösen. Hier ein paar Beispiele für einzelne Stufen:

- Malware wird über einen E-Mail-Anhang oder eine infizierte Website installiert.
- Ein offener Kommunikationskanal wird eingerichtet (die so genannte „Backdoor“), in der Regel ein Trojaner.

- Zusätzliche Malware wird heruntergeladen und kann die Form der ursprünglichen Malware verändern.

Es sind verschiedene Varianten von Bedrohungen in unterschiedlicher Anzahl enthalten:

- **Variantenvielfalt:** Zahllose Pakete mit einer kleinen Anzahl an Bedrohungen, die als Varianten erzeugt werden. Die Vielfalt ist ein Versuch, der Entdeckung immer einen Schritt voraus zu sein.
- **Protokollvielfalt:** Angriff auf mehr als ein System. Eine Bedrohung wird beispielsweise über einen Link in einer E-Mail übertragen, sucht nach Schwachstellen im Browser oder greift über eine E-Mail bzw. IM-Protokolle an.
- **Verteilung:** Verbreitung des Schadteiles über viele Hosts, auch hier in eher kleiner Anzahl.

Die Kombination von Angriffsmethoden kann fatal sein: Mit Spam können unzählige Empfänger erreicht werden, das Internet ist das perfekte Massenmedium und mit Malware wird der Schadteil ausgeführt. Jede Komponente für sich mag harmlos erscheinen, doch das Gesamtbild zeigt den kombinierten Angriff in aller Deutlichkeit.

Social-Engineering-Techniken bekämpfen

Letztes Jahr haben Kriminelle zunehmend *Social-Engineering-Techniken* (eigentlich „Cyber-Lügen“) angewendet, um ihre betrügerischen Ziele zu erreichen. Sie stützen sich dabei auf Themen, die in der Presse kursieren, oder geben vor, Mitarbeiter Ihrer Bank oder einer Ihrer Lieferanten zu sein, um Sie zum Öffnen von Malware zu verleiten. Sie verwenden Phishing-Mails, um dem Benutzer persönliche Daten zu entlocken. Dabei werden Sie zum Beispiel aufgefordert, einen Fragebogen für eine Studie auszufüllen, der eine Prämie verspricht. Andere geben vor, ein Kontaktnetzwerk oder sogar ein Antiviren-Anbieter zu sein.

Am allerschlimmsten aber ist, dass sich diese Bösewichte nicht nur auf die virtuelle Welt beschränken. Auch im realen Leben wird versucht, Menschen auf infizierte Websites zu locken. Ein Beispiel hierfür sind Flugblätter an Autos auf

Parkplätzen: Der betreffenden Person drohe eine Geldbuße wegen Falschparkens. Daher solle sie ihre Fahrzeugangaben auf einer bestimmten Website bestätigen. Beim Öffnen der Website wird dann Malware auf dem Computer installiert.

Ein raffinierter Trend bei Spam ist das so genannte *Backscatter*: Kriminelle versenden Massen-Mails an eine große Anzahl von Empfängern und täuschen dabei einen anderen Absender vor. Der Besitzer des als Absender vorgetäuschten E-Mail-Kontos erhält dann zahllose E-Mails zu nicht erfolgter Zustellung oder automatische Abwesenheitsmeldungen.

Fallstudie einer Internet-Bedrohung: der Conficker-Wurm

Der Conficker-Wurm bzw. WORM_DOWNAD ist ein gutes Beispiel dafür, wie Cyberkriminelle die herkömmlichen Taktiken von Massenausbrüchen mit moderneren, komplexen Angriffsmechanismen und einer C&C-Infrastruktur (Command & Control) kombinieren.

Der Wurm nutzte nämlich eine Schwachstelle in einem Windows Dienst aus, um Windows Computer zu infizieren. Anschließend verbreitete er sich über Windows Netzwerke. Einer darauf folgenden Variante gelang es, in Netzwerkserver und Wechsellaufwerke einzudringen und dadurch bereits schon einmal infizierte Computer erneut zu infizieren. Der Conficker-Wurm gilt als der am weitesten verbreitete Wurm seit SQL Slammer aus dem Jahr 2003: Bis Januar 2009 infizierte er zwischen 9 und 15 Millionen Computer.

Der Wurm sperrt den Zugriff auf die Website von Antiviren-Anbietern, deaktiviert Windows Updates sowie andere Windows Dienste und sperrt Benutzerkonten. Er erzeugt eine Liste mit Domain-Namen, mit denen er sich verbindet und von denen er weitere Schadteile herunterlädt.

Im Oktober 2008 veröffentlichte Microsoft einen Notfall-Patch, um diese Schwachstelle auszubessern, und setzte eine Notfall-Arbeitsgruppe ein, um die schädlichen Auswirkungen von Conficker zu bekämpfen. Die Gruppe bot eine Belohnung von 250.000 Dollar für Hinweise, die zur Festnahme der Urheber führen. Auf vielen Geräten wurden die Fehler aber nicht behoben.

Viele Spekulationen gab es um den schlussendlichen Schadteil, als das Bot-Netz des Wurms am 1. April 2009 erneut an den Start ging. Allerdings war der verursachte Schaden zum Zeitpunkt, als dieses Buch geschrieben wurde, nur begrenzt.

. . . und es werden immer mehr

Die Menge der heutzutage erzeugten Malware wächst dramatisch. Dem Unternehmen AV-Test zufolge gab es 1988 1738 unterschiedliche Bedrohungsmuster. Bis 2005 kamen *jedes Jahr* mehr als doppelt so viele dazu. Doch in den letzten paar Jahren ist die Anzahl der Bedrohungen geradezu explodiert. Im Folgenden finden Sie einige statistische Daten, die Sie verblüffen werden:

- Anfang 2008 überstieg die Gesamtzahl vorhandener Bedrohungen die 10-Millionen-Grenze. Ende 2008 hatte diese Zahl die 20-Millionen-Grenze erreicht – in weniger als einem Jahr hatte sie sich gewissermaßen verdoppelt!
- Im Durchschnitt erreichen pro Stunde über 2000 neue Malware-Bedrohungen das Internet.
- In weniger als einer Woche kann heutzutage die gesamte Malware von 2005 erzeugt werden.

In bestimmten Sparten gab es 2008 einen massiven Anstieg von Spam und Bots: Diese beiden Bedrohungstypen sind miteinander verzahnt, da Bot-Netze zu den Hauptverursachern von Spam zählen. Von Januar bis November 2008 wurde die schwindelerregende Summe von 34,3 Millionen Computern mit Malware infiziert, und zwar von Quellen, die häufig mit Bots in Verbindung gebracht werden.

Gestatten? Die cyberkriminelle Unterwelt

Im Gegensatz zur allgemeinen wirtschaftlichen Lage befindet sich die cyberkriminelle Wirtschaft im Aufschwung. Schätzungen zufolge setzt die cyberkriminelle Unterwelt pro Jahr mittlerweile über 100 Milliarden Dollar um. Da die Einsätze immer höher werden, wird die Unterwelt zunehmend professioneller und ähnelt in ihrer Struktur immer mehr einem Unternehmen. Das bedeutet also, dass sich bestimmte Leute darauf spezialisieren, Stördienste anzubieten. Mittlerweile kann man fast alles kaufen oder mieten.

Neben den im Paket angebotenen Optionen können Cyberkriminelle auch regelrechte Malware-Schreiber

beauftragen, die im Internet Code verkaufen – eben genauso wie echte Software-Entwickler.

Um wie viel Geld geht es?

Mit gestohlenen Informationen lässt sich viel Geld machen: Cyberkriminelle handeln mit persönlichen Daten, einschließlich E-Mail-Anmeldedaten, Kreditkartennummern, Sozialversicherungsnummern, Bankverbindungen und Kennwörtern für Spiele. Cyber-Kriminelle machen krumme Geschäfte mit Bot-Netz-Anbietern und Hackern, handeln mit Malware-Anbietern, die wiederum mit Anti-Detection-Anbietern und Toolkit-Herstellern zusammenarbeiten. Kreditkartenbetrüger, Spammer und Erpresser arbeiten parallel und manchmal zusammen mit diesen unabhängigen Geschäftsleuten in einer immer stärker miteinander verknüpften Branche.

Mittlerweile sind die Preise auf dem Cyber-Schwarzmarkt erstaunlich günstig geworden. Laut einem Artikel in der britischen Zeitung *The Independent* erhält man für 50 bis 3.500 Dollar „Malware von der Stange". Für 25 bis 60 Dollar monatlicher „Abo-Gebühren" bekommt man einen Dienst, der Antiviren-Entwicklungen und Malware-Verbesserungen beobachtet. Dem Artikel zufolge muss man mit einem Stundenpreis von ungefähr 200 Dollar rechnen, um ein Bot-Netz mit 8.000 bis 10.000 Computern zu nutzen. Nachforschungen von TrendLabs zur digitalen Untergrundwirtschaft im Jahr 2007 kamen unterdessen zu dem Ergebnis, dass man für nur 100 Dollar am Tag einen verteilten DoS-Angriff und für 1.000 Dollar 10.000 infizierte Computer einkaufen kann. DoS-Angriffe zielen darauf ab, Online-Ressourcen außer Betrieb zu setzen, und zwar indem sie diese mit Dienstanfragen bombardieren.

Mit vielen Tools zum Ziel

Einer der Gründe für den zunehmenden Erfolg Cyberkrimineller ist die Verfügbarkeit von Werkzeugen, die ihnen helfen, ihre Aktivitäten zu starten. Diese Tools reichen von kostenlosen vorgefertigten Phishing-Kits von jemandem wie „Mr Brain" (eine Gruppe marokkanischer Betrüger, die einfach verwendbare Kits anbieten und viele führende Banken angegriffen haben) bis hin zu kostenlosen Spam-Vorlagen, die die Website bekannter Banken täuschen ähnlich nachmachen.

Datenmissbrauch nimmt zu: Laut dem Missbrauchsbericht 2008 des Identity Theft Resource Center wurden Ende 2008 656 Fälle von Datenmissbrauch gemeldet, ein Anstieg von 47 Prozent gegenüber der Gesamtsumme von 446 Fällen im Jahr 2007. Die Gesamtzahl liegt bei 35 Millionen gefährdeten Datensätzen.

Gleichermaßen beunruhigend ist der Anstieg von Programmen zur automatischen Erstellung von Malware: Mit nur einer Malware-Instanz können sie Hunderte von Varianten mit einem unverwechselbaren Profil erzeugen und entgehen dadurch der herkömmlichen, auf Pattern-Dateien basierenden Entdeckung.

Kapitel 5

Praktische Lösungen ausarbeiten

In diesem Kapitel geht es um

- Das Gefühl, von der steigenden Bedrohungsflut überschwemmt zu werden
- Die Konfrontation mit Bedrohungen aus allen Richtungen
- „Cloud Computing“: Der Schutz liegt in der Wolke
- Die Verbindung zum „Smart Protection Network“

Da sich die Anzahl der IT-Bedrohungen jedes Jahr exponentiell erhöht, scheinen die Anbieter von Sicherheitslösungen manchmal ähnlich dem dänischen König Knut zu versuchen, das Meer zurückzuhalten. Obwohl die meisten Unternehmen verstehen, dass IT-Sicherheit wichtig ist, und die Maßnahmen aus Kapitel 3 umsetzen, werden herkömmliche Schutzvorrichtungen in der Zukunft nicht mehr ausreichen.

Pattern-File-Updates – Erklärung folgt – werden nicht nur umfangreicher und häufiger, sondern auch immer weniger effektiv, da Cyberkriminelle ihre Angriffe ununterbrochen abändern und komplexe Internet-Bedrohungen verwenden, um ihre Absichten zu verbergen.

Hier tritt das so genannte „Cloud Computing“ als Retter der IT-Sicherheit auf den Plan. Es handelt sich um einen Ansatz, der schon für andere Lösungen verwendet wird, die eine große Datenmenge extern speichern und permanent aktualisieren müssen. Außerdem reduziert dieser Ansatz den Verwaltungsaufwand für kleine Unternehmen ganz erheblich.

Das Smart Protection Network, zu dem wir später noch kommen, geht einen Schritt weiter. Es übernimmt zwar den Cloud-Computing-Ansatz, verbindet dann aber alle Clouds miteinander. Diese Art der Ressourcenteilung ist für die EDV von heute unumgänglich als eine Art Nachbarschaftswache für die IT-Sicherheit.

Der vergebliche Kampf gegen die Fluten

Die Malware-Menge ist in den letzten Jahren dramatisch gestiegen. In den kommenden Jahren wird es aber nur noch schlimmer. TrendLabs hat zwischen 2005 und 2008 einen Anstieg von 1.731 Prozent bei eingehenden Bedrohungen beobachtet und prognostiziert für 2015, dass es 26.598 Bedrohungen pro Stunde verarbeiten wird (siehe Abbildung 5-1).

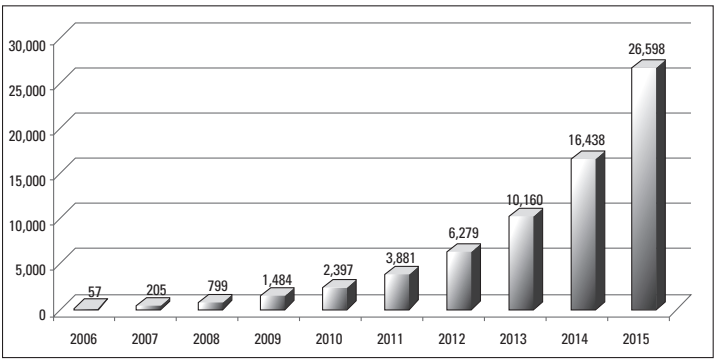


Abbildung 5-1: Der prognostizierte Anstieg eingehender Malware-Bedrohungen.

Der Grund, warum sich Analysten so sicher sind, dass die Malware-Flut unvermindert anwachsen wird, ist der Teufelskreis, in dem Computernetze gefangen sind. In den USA zum Beispiel wächst die Malware-Flut trotz erheblicher Aktivitäten und regulierender Maßnahmen im Kampf gegen Spam weiter an, da ständig neue Spam- und Phishing-Aktivitäten auftauchen. Die USA sind hier noch immer einsamer Spitzenreiter und verbuchen über 22,5 Prozent aller Spam-Mails. Der unaufhaltsame Anstieg von Bots wird zu noch mehr Spam, DoS-Angriffen und anderen IT-Angriffen führen.

Der McColo-Effekt

Sollten Sie weitere Beweise für den permanenten Anstieg von Bedrohungen brauchen, finden Sie diese im Fall McColo aus dem Jahre 2009. McColo Corp war ein in San Jose ansässiger Internet-Hosting-Provider, dem man nachsagte, alle möglichen Arten cyberkrimineller Anwender zu beherbergen, und zwar von Spammern bis zur C&C-Infrastruktur einiger der weltweit größten bekannten Bot-Netze. Diese Bot-Netze kontrollierten Tausende von Computern, die in Spam, Malware, Kinderpornografie, Kreditkartendiebstahl, Betrug und den „Masche zum schnellen Geld"-Fallen verwickelt waren.

Nach jahrelangen Ermittlungen wurde McColo im November 2008 endlich abgeschaltet. Über Nacht sank die Anzahl der Junk-Mails weltweit 50 bis 75 Prozent. Diese positive Wirkung hielt allerdings nicht lange an: Das Spam-Aufkommen stieg allmählich wieder an, und eines der größten Bot-Netze, das McColo gehostet haben soll, scheint immer aktiver zu werden, wird allerdings von einer anderen Stelle aus gesteuert.

Signaturdateien können nicht mithalten

Die massenhafte Ausbreitung von Bedrohungen erschwert es herkömmlichen Schutzmaßnahmen, wie zum Beispiel Pattern-Datei- und Signatur-Updates, Schritt zu halten. Die meisten modernen Antiviren-Systeme fahnden nach Viren, indem sie Computer nach einem bestimmten Muster durchsuchen und es mit einer Pattern-Datenbank abgleichen, die sie gespeichert haben. Sobald eine übereinstimmende Signatur gefunden wird, wird die fehlerhafte Datei in Quarantäne verschoben oder gleich vollständig gelöscht.

1988, als es nur 1.738 verschiedene Bedrohungsmuster gab, teilten die Fachleute diese schlicht in 30 Familien (oder Pattern) ein und mussten nur 30 Signaturen herausgeben, die ihre Scanner mit der Malware verglichen. Nur vereinzelt tauchten vollkommen neue Pattern auf, nämlich dann, wenn die Virenschreiber eine neue Methode gefunden hatten, um ihren Schadteil zu verbreiten.

Heute gibt es stündlich Tausende neuer Pattern. Cyberkriminelle wissen, inwieweit das Veröffentlichen von Pattern-Updates den Handlungsspielraum der Antiviren-Anbieter einschränkt, und erzeugen ständig neue Varianten ihrer Malware. Oft verändern sie die Malware innerhalb weniger Stunden nach der ersten Veröffentlichung, um die Nase auch weiterhin vorn zu haben.

Die Sicherheitsbranche hat auf dieses Problem mit der häufigeren Veröffentlichung von Updates reagiert. Einige Anbieter aktualisieren ihre Sicherheitsmaßnahmen zweimal täglich oder sogar stündlich. Jedes neue Update enthält noch mehr Pattern, da die Antiviren-Anbieter so versuchen, die Flut von Internet-Bedrohungen einzudämmen.

Häufige Pattern-DateiUpdates haben ihren Preis. Sie können:

- beim Update der Client-Geräte einen großen Teil der Netzwerk-Bandbreite beanspruchen,
- die Leistungsfähigkeit einzelner Computer herabsetzen,
- dem Netzwerk-Administrator zusätzliches Kopfzerbrechen bereiten, da er überprüfen muss, ob auch alle Geräte aktualisiert wurden.

Häufigkeit und Menge der Pattern-Updates überlastet Firmennetzwerke, verschwendet wertvolle Bandbreite, die eigentlich für wichtige geschäftliche Aufgaben gedacht ist, und verringert die Leistungsfähigkeit der Computer. Wenn Sie morgens Ihren Computer hochfahren und eigentlich sofort mit der Arbeit beginnen wollen, gibt es nichts Ärgerlicheres als zu warten, bis der Computer ein Update beendet hat.

Komplexen Bedrohungen die Stirn bieten

Es scheint Anzeichen dahingehend zu geben, dass sich die Sicherheitsmaßnahmen von Unternehmen und der Schutz ihrer Geschäftstätigkeit verbessert. Zum Beispiel fand eine Studie zu Informationssicherheitslücken heraus, dass von allen Unternehmen:

- 99 Prozent kritische Systeme und Daten sichern.
- 98 Prozent über Software verfügen, die nach Spyware sucht.
- 97 Prozent eingehende E-Mails nach Spam filtern.
- 97 Prozent ihre Website durch eine Firewall schützen.
- 95 Prozent eingehende E-Mails auf Viren überprüfen.
- 94 Prozent über das drahtlose Netzwerk gesendete und empfangene Informationen verschlüsseln.

Dabei sind es nicht nur die technischen Kontrollen, die sich verbessert haben. Die Studie fand außerdem heraus, dass 55 Prozent aller Unternehmen über eine durch Unterlagen belegte Sicherheitsrichtlinie verfügen (im Jahr davor lag diese Zahl noch bei nur 27 Prozent) und 40 Prozent fortlaufend Mitarbeiter-Trainings zum Thema Sicherheitssensibilisierung anbieten (20 Prozent mehr als im Jahr davor).

Diese Zahlen beziehen sich vor allem auf größere Unternehmen, die über mehr Betriebsmittel für Sicherheitskontrollen, Dokumentation und Sensibilisierungsmaßnahmen verfügen. Nichtsdestotrotz machen diese Zahlen Mut.

Dazu kommen noch Mehrfachbedrohungen

Herkömmliche IT-Sicherheitsmaßnahmen bekämpfen die herkömmlichen Herausforderungen der IT-Sicherheit. Wie sieht es aber mit den neueren Bedrohungen aus, die diese technischen Kontrollen umgehen? Da ist zum Beispiel die *datenstehlende Malware*, die Firmennetzwerke infiziert und unentdeckt Unternehmensdaten entwendet, um diese für Betrügereien zu verwenden. Datenstehlende Malware ist eine Form komplexer Internet-Bedrohung, die in der Regel aus einer ganzen Reihe von Bedrohungen besteht. Scheinbar harmlosen Aktivitäten werden hier mit einem Schadteil kombiniert, wie in Abbildung 5-2 dargestellt.

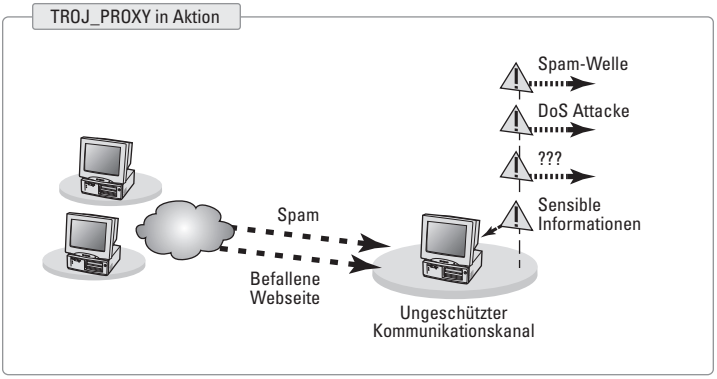


Abbildung 5-2: Eine komplexe Internet-Bedrohung aus Spam und bösartigen Websites.

Komplexe Internet-Bedrohungen können sich von einem harmlos wirkenden Programm in etwas Bösartiges verwandeln, wodurch sie den dateibasierten Virensuchvorgang umgehen. Oft gelangen sie entweder über den offenen Internet-Protokoll-Port ins System, schlagen also dem IDS (z. B. eine Firewall) ein Schnippchen, oder aber über einen Link in einer E-Mail.

Der E-Mail-Filter durchsucht zwar alle E-Mail-Anhänge, doch wenn ein Benutzer dazu gebracht werden kann, auf einen Link zu klicken, öffnet sich dadurch eine betrügerische Website, die der Cyberkriminelle betreibt. Von dieser Seite wird dann Malware heruntergeladen.

Außerdem dehnen Cyberkriminelle ihre Reichweite immer mehr aus und zielen auch auf Mobiltelefone ab – besonders auf Windows Mobile Pocket PC und die Betriebssysteme von Symbian und Palm. Der zunehmende Einsatz dieser Geräte im geschäftlichen Umfeld wird den Systemadministratoren noch eine ganz neue Art von Kopfzerbrechen bereiten.

Cyberkriminelle testen ihre neue Malware ständig an dateibasierten Antiviren-Produkten, und ihre Angriffe sind so effektiv, dass sie von vielen Produkten einfach nicht entdeckt werden. Da die Bedrohungen unaufhörlich ihre Angriffsmuster variieren, ist eine Signatur- oder verhaltensbasierte Überprüfung unwirksam.

Gefahr droht aus dem Web

Unternehmens-Websites werden von Cyberkriminellen immer häufiger mit automatischen Tools angegriffen, die das Internet systematisch nach Sicherheitslücken durchforsten (Stichwort „Crawler“).

Umfangreiche Websites wie eBay und Google sind davon natürlich überproportional häufig betroffen, aber Cyberkriminelle holen auch aus der Website eines kleineren Unternehmens jede Menge Informationen heraus. Hierbei handelt es sich oft um ältere Websites, deren Tools und Software nicht auf den neuesten Stand sind – und dies wiederum, weil dem Unternehmen die Ressourcen fehlen, um Tools und Software zu aktualisieren.

Immer mehr Websites werden infiziert. Die neuesten Zahlen von White Hat Security zeigen, dass 64 Prozent aller Websites eine hohe Anfälligkeit bzw. eine kritische Sicherheitslücke aufweisen, während laut Websense 70 Prozent der am häufigsten aufgerufenen 100 Websites bösartigen Content oder eine versteckte Umleitung enthalten.

Angesichts derartig alarmierender Infektionsraten ist es heute eine der größten Herausforderungen für die Sicherheitsbranche, den Überblick über betroffene, geografisch weit verteilte Websites zu behalten.

Sicherheit in der Web-Wolke finden

Unter *Cloud-Computing* versteht man einen Pool gemeinsam genutzter IT-Ressourcen, der in der Regel (Ausnahme: große Unternehmen) nicht am Unternehmensstandort gespeichert wird. Cloud-basierte Services beinhalten zum Beispiel gehostete E-Mail-Sicherheit sowie gehostete Web-Reputation und File-Reputation-Datenbanken. In diesen Speichern sind die Informationen über zweifelhafte Websites und Dateinamen enthalten. Weitere Informationen zum Thema „Hosting-Services“ finden Sie in Kapitel 2. Die Pattern-Datei-Datenbanken und andere Sicherheitsressourcen in das Internet, also die Cloud, zu verlegen, ist eine Lösung, um dem Problem der massiv steigenden Anzahl von Bedrohungen zu begegnen.

Der Vorteil des Cloud-Computings liegt darin, Fachleuten die Verwaltung des großen Ressourcenpools zu überlassen, um diesen internen Aufwand zu sparen. Darüber hinaus ist Cloud-Computing:

- Skalierbar und kann problemlos mitwachsen, wenn Sie mehr Ressourcen hosten lassen wollen.
- Virtualisiert, was mit anderen Worten heißt, dass es die IT-Ressourcen, auf denen es betrieben wird, bestmöglich nutzt und daher weniger Ressourcen verbraucht.
- Zuverlässiger, da Sie sich hinsichtlich der Updates nicht auf Ihr eigenes Netzwerk verlassen müssen. Solange Sie eine Internet-Verbindung haben, können sich Ihre Computer automatisch selbst aktualisieren.
- Günstiger als eine lokale Installation der Ressourcen, obwohl die Kosten von der Anzahl der Benutzer und der Größe der von Ihnen verwendeten Datenbank abhängen.
- Endpunkt-übergreifend wirksam, so dass Sie Ihre mobilen Mitarbeiter, unterschiedlichen mobilen Geräte etc. problemlos verbinden können, ohne selbst ein Gerät nach dem anderen manuell aktualisieren zu müssen. Dadurch hängt Sicherheit nicht mehr von einem bestimmten Ort ab.
- Sicherer. Es hat zahlreiche Diskussionen über die Sicherheit von Cloud-Computing-Systemen gegeben. Der klare Vorteil: Der Sicherheitsanbieter hostet seine eigene Software, anstatt dass Sie versuchen, diese Software auf Ihrem System laufen zu lassen. Die Software liegt jetzt zwar nicht mehr in Ihrer Kontrolle, aber dafür ist es sicherer.

Durch die Ausführung der Sicherheitslösung in der Cloud lassen sich unterschiedliche Cloud-Services miteinander verbinden, sodass diese untereinander kommunizieren. Dies bekämpft komplexe Internet-Bedrohungen, da die Bedrohungs-Pattern innerhalb der einzelnen Angriffskomponenten erkannt werden. Hier tritt das Cloud-Computing als Retter der IT-Sicherheit auf den Plan.

Das Smart Protection Network erkunden

Das Smart Protection Network ist ein neuer Ansatz, der die neuesten Technologien nutzt.

Da die Sicherheitsressourcen an ihre Grenzen stoßen und die Situation zunehmend schwieriger wird, wurde die dynamische Echtzeit-Technologie des Smart Protection Network dazu entwickelt, gemäß der Art der Bedrohung zu skalieren und Netzwerk sowie Computer-Ressourcen weniger zu belasten als herkömmliche Produkte.

Ein webbasiertes Smart Protection Network besteht aus drei Elementen:

- E-Mail Reputation schätzt die Authentizität von E-Mail-Adressen basierend auf ähnlichen gespeicherten Adressen ein,
- Web Reputation (oder Schutz vor Internet-Bedrohungen),
- File Reputation (oder intelligente Suche).

Sie erhalten:

- Einen vernetzten Abgleich zwischen den Ereignissen: Enthält eine Spam-Mail einen Link zu einer bestimmten Website, kann dieser Link zur Schwarzen Liste hinzugefügt werden. Dadurch wird die Malware, die sich hinter dieser Website verbirgt, analysiert, mit einer Signatur versehen und gestoppt.
- Weltweit vernetzte Datenbanken: Informationen zu Sicherheitslücken in Asien oder Europa werden weltweit aktualisiert.
- Eine Feedback-Schleife aus einzelnen Benutzern, die gewissermaßen alle Informationen über die Bedrohung, mit der sie konfrontiert sind, miteinander teilen.

Der Sicherheitsanbieter unterhält das globale Netzwerk mit den Bedrohungsdaten, wobei er jeden Tag Millionen verdächtiger IP-Adressen, URLs und Dateien hinzufügt. Und weil es sich um ein gehostetes Netzwerk handelt, können

täglich Milliarden von Anfragen bearbeitet werden. Dieses Netzwerk bietet somit umfassenden Schutz vor allen Arten von Bedrohungen, einschließlich der neuartigen Internet-Bedrohungen.

Die Korrelation ist beim Kampf gegen komplexe Bedrohungen ein wichtiges Instrument. Es ist die Kombination der drei oben definierten Elemente, die das Smart Protection Network bei der Bekämpfung von Internet-Bedrohungen so effektiv macht. Das Netzwerk ist in der Lage, zwischen verschiedenen Ereignissen eine Verbindung herzustellen, kann dadurch ein globales Bild aufbauen und letztendlich die Bedrohungsdatenbank optimieren.

Ein Smart Protection Network verwendet weltweite Feedback-Schleifen, um eine Sicherheitsbedrohung zurückzuverfolgen und ihre Ursache zu finden. Dabei vernetzt es Forschungszentren, Benutzer, Produkte und Services:

- Wenn eine Malware entdeckt wird, erzeugt das Netzwerk eine Feedback-Meldung, woraufhin der ursprüngliche Link ermittelt und das Smart Protection Network dementsprechend aktualisiert wird.
- Jede E-Mail mit diesem Link wird in Zukunft am Netzwerk-Gateway gesperrt, weil eben dieser Link sich jetzt auf der Schwarzen Liste der Web Reputation Datenbank befindet.
- Weitere Downloads werden gestoppt, da das Datei-Pattern zur File-Reputation-Datenbank hinzugefügt wird, wodurch die Infektionskette zum frühestmöglichen Zeitpunkt unterbrochen wird.

Die Cloud liefert schnellere Ergebnisse, da die Wartezeit entfällt, bis der Computer die neuesten Pattern-File-Updates heruntergeladen hat.

Ein Smart Protection Network wird manchmal mit einer virtuellen Version der Nachbarschaftswache verglichen, bei der alle Nachbarn wachsam sind und Probleme abwenden, bevor sie eintreten.

Ein Blick in die Zukunft der IT-Sicherheit

In Zeiten, in denen die Sicherheitsressourcen an ihre Grenzen stoßen und die Situation zunehmend schwieriger wird, weist die Kombination aus webbasierten und herkömmlichen Technologien den Weg in die Zukunft der IT-Sicherheit. In Tests hat sich diese Kombination als der beste Schutz erwiesen.

Beim Vergleich mit neun anderen Lösungen hatte zum Beispiel die gehostete E-Mail-Sicherheitslösung in einem Anti-Spam-Vergleichsbericht von West Coast Labs im Januar 2009 die höchste Erkennungsrate (96,71 Prozent) sowie eine zu vernachlässigende Menge an Fehlalarmen.

Ein weiteres Beispiel ist der von NSS Labs im November 2009 durchgeführte Test der neuesten Sicherheitslösungen. Hier wurde die Wichtigkeit einer Kombination aus Cloud- und Client-Schutz (lokal gehostet) unter Beweis gestellt, wobei der Sieger in 96,4 % der Fälle Schutz gegen reale Bedrohungen von heute bot.

Eines nicht allzu fernen Tages werden unterschiedliche Technologien und Ansätze vereint sein und den Weg in die Zukunft der IT-Sicherheit weisen. Für kleine Unternehmen bedeutet dies, dass ihre Vermögenswerte sicherer sind und dass die Verwaltung ihrer Sicherheitslösung einfacher, erschwinglicher und unkomplizierter wird.

Kapitel 6

Die 10 besten IT-Sicherheitsmaßnahmen für kleine Unternehmen

In diesem Kapitel

- Erfahren Sie, womit Sie es zu tun haben
- Lernen Sie Wege kennen, die Bedrohungen zu bekämpfen

Dieses kurze Kapitel bietet die wichtigsten Methoden, die ein kleines Unternehmen braucht, damit seine IT-Sicherheitslösung wirksam genutzt wird. Wir sind sicher, dass Ihr Unternehmen alle zehn Punkte umsetzt!

Bedrohungen ermitteln

Jedes Unternehmen mit Internet-Verbindung – eigentlich jede Person mit einem Internet-Anschluss – wird irgendwann das Opfer von Cyberkriminellen. Um Ihre Technologie und Ihr Unternehmen rundum zu schützen, müssen Sie herausfinden, welche Bedrohungen die größten Probleme verursachen. Kapitel 1 hilft Ihnen, die Vorfälle zu bestimmen, die Ihrem Unternehmen und seinem Fortbestehen schaden könnten.

Negative Auswirkungen analysieren

Nachdem Sie die Bedrohungen für Ihr Unternehmen ermittelt haben, müssen Sie den möglichen Schaden bestimmen, falls diese Bedrohungen Wirklichkeit werden. Gehen Sie alle „Was wäre wenn"-Szenarien durch, die Ihnen einfallen, damit Sie sich überlegen können, wie Ihr Unternehmen wiederhergestellt wird, falls diese Szenarien eintreten. Kapitel 1 hilft Ihnen dabei, diese Analyse durchzuführen.

Eine Sicherheitsrichtlinie abfassen

Die Maßnahmen, die Sie zum Schutz Ihres Unternehmens treffen, bilden die Sicherheitsrichtlinie, die den Leitfaden für die Geschäftspraktiken und das Mitarbeiterverhalten darstellt. Kapitel 2 behandelt dieses Thema in allen Einzelheiten.

Vermögenswerte und deren Risikofaktoren ermitteln

Sie müssen Ihre Vermögenswerte kennen, um einen Weg zu finden, sie zu schützen. Das Abschätzen der Risiken für jeden Vermögenswert hilft Ihnen, geeignete Schutzmaßnahmen zu finden.

Allgemeine Nutzungsrichtlinien abfassen

Ihr Unternehmen stellt die Tools bereit, die Ihre Mitarbeiter für ihre Arbeit benötigen. Ihre Mitarbeiter müssen in Bezug auf jedes einzelne Tool wissen, was man unter einer zulässigen bzw. unzulässigen Nutzung versteht. Zum Beispiel müssen Sie Ihren Mitarbeitern den Besuch von Websites

untersagen, die sowohl den Mitarbeiter als auch Sie mit dem Gesetz in Konflikt bringen könnten. Wie in Kapitel 2 erklärt, sollten Sie allerdings nicht nur die illegale sondern jede Art von Nutzung einschränken, die die Produktivität und angemessene Geschäftsmethoden beeinträchtigt.

Eine Internet- und E-Mail-Richtlinie abfassen

Zwei der wichtigsten Instrumente, die Sie Ihren Mitarbeitern zur Verfügung stellen, sind der E-Mail-Zugang und das Internet. Eine diesbezügliche Richtlinie gibt Ihren Mitarbeitern einen Leitfaden zur ordnungsgemäßen und unternehmensbezogenen Nutzung dieser Tools. Vorschläge dazu finden Sie in Kapitel 2.

Technische Kontrollen einrichten

Jedes Unternehmen muss über bestimmte Systeme verfügen, um seine IT-Funktionen zu schützen. Stellen Sie sicher, dass Sie das Wesentliche abdecken, indem Sie eine Firewall installieren und eine Antiviren-/Anti-Spam-Software erwerben. Kapitel 3 beschäftigt sich mit Abwehrmaßnahmen.

Sicherheitselemente koordinieren

Es gibt eine Reihe von Sicherheitsmaßnahmen, mit denen Sie eine Reihe von Schwachstellen schützen können. Alle diese Sicherheitskontrollen müssen zusammen mit den Richtlinien für die Mitarbeiter einen gemeinsamen Schutzschild für Ihr Unternehmen bilden. In Kapitel 3 finden Sie weitere Informationen zu diesem Thema.

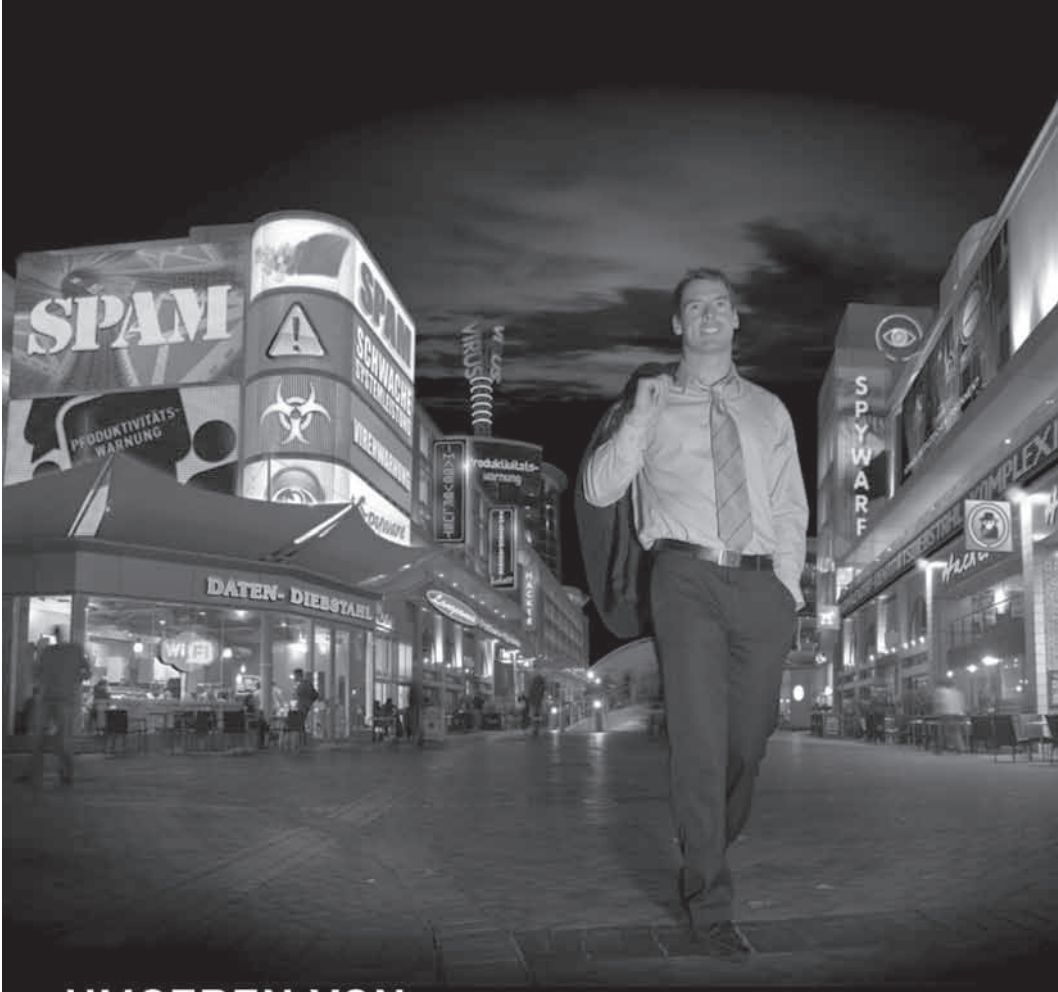
Kenne deinen Feind

Sie müssen die Vorgehensweise von Cyberkriminellen kennen. Außerdem müssen Sie einen Überblick über die neu auftretenden Bedrohungen, wie zum Beispiel komplexe

Bedrohungen, behalten, damit Sie Ihre Mitarbeiter darüber aufklären können, wie mit diesen Bedrohungen zu verfahren ist. Die neuesten Tipps und Bedrohungen finden Sie in Kapitel 4.

Nutzen Sie das Potenzial des Cloud-Computing

Das Cloud–Computing ermöglicht Ihnen die gemeinsame Nutzung von Ressourcen eines Datenzentrums. Sie profitieren von besserem Schutz sowie von geringeren Beeinträchtigungen Ihres Netzwerk und Ihrer Computer-Ressourcen. In die Wolke geht es im Kapitel 5.



UMGEBEN VON INTERNET-BEDROHUNGEN TUT ES GUT, SORGENFREI ZU SEIN.

Sicherheitsbedrohungen verfolgen uns heute auf Schritt und Tritt. Alle 2 Sekunden wird ein neuer Virus entdeckt. Darum ist es heute wichtiger denn je, die Produktivität und den guten Ruf mit Trend Micro™ Worry-Free™ Business Security zu schützen.

Diese vom Smart Protection Network unterstützte Sicherheitslösung entdeckt Bedrohungen bereits im Internet und macht sie unschädlich, bevor sie Ihr Unternehmen erreichen. Die Lösung entlastet Ihr Netzwerk, und Sie können sich um Wichtigeres als die Sicherheitsverwaltung kümmern.

DIE ZEICHEN ERKENNEN
Holen Sie sich noch heute Ihre kostenfreie Testversion unter www.trendmicro.de/worry-free-finder

TREND MICRO™
Securing Your Web World

Fakten von Fiktion unterscheiden

Sicher gegen IT-Bedrohungen

IT-Sicherheitsbedrohungen sind überall, und es scheint, als würden jeden Tag neue hinzukommen. Kleine Unternehmen haben allerdings nur beschränkte Mittel zur Verfügung, um ihre Vermögenswerte zu schützen. Dieses Buch bietet Ihnen die wesentlichen Grundlagen für einen effektiven Schutz Ihres Unternehmens. Es gibt einen Überblick über die größten IT-Bedrohungen sowie deren negative Auswirkungen auf Ihr Unternehmen, und hilft Ihnen, eine Sicherheitsrichtlinie zu erstellen, ein koordiniertes Abwehrsystem einzurichten und – was am wichtigsten ist – Ihre Sicherheit besser zu verwalten. Cyberkriminelle erfinden beständig neue Angriffsmöglichkeiten – hier lernen Sie, wie Sie den zunehmenden Ansturm eindämmen können.

Lernen Sie:

- *eine Sicherheitsrichtlinie zu schreiben*
- *Ihr Abwehrsystem zusammenzufügen*
- *die wachsenden Bedrohungen zu bekämpfen*

SO SIND DIE DUMMIES™

- *Erklärungen ohne Fach-Chinesisch*
- *Tipps und Tricks zum Ausprobieren*
- *Symbole helfen zu verstehen*
- *Praktischer Spickzettel*
- *Top-Ten-Listen*
- *Eine Prise Humor und Spaß*

Machen Sie sich schlau!

www.fuer-dummies.de

- *Hier finden Sie alle unsere Bücher für Dummies*
- *Wählen Sie aus vielen verschiedenen Themengebieten*
- *Download von Probekapiteln, Inhalts- und Stichwortverzeichnissen*

ISBN: 978-0-470-66692-0

Für Dummies®
Eine Marke von WILEY