

Executive Brief

IT Security - Trends und Anwenderpräferenzen

Deutschland 2010

.....

Gesponsort von Kaspersky Lab

.....

EINLEITUNG

IT Security ist in den IT-Abteilungen deutscher Unternehmen das vorherrschende Thema. Seit Jahren steht das Thema der Absicherung der eigenen IT vor Bedrohungen weit oben auf der Agenda von IT-Verantwortlichen.

Allerdings wird das Thema IT Security immer komplexer und aufwendiger. Die Unternehmens-IT ist schon jetzt keine "Festung" mit definierten fixen Ein- und Ausgängen mehr, die es zu verteidigen gilt, sondern ein loses Gebilde, in dem die Grenzen zunehmend verschwimmen, z.B. durch mobile Endgeräte oder Web 2.0 Technologien. Cloud Services werden diesen Trend noch verschärfen. Vor allem Web 2.0 stellt eine enorme Herausforderung in Bezug auf Data Loss Prevention (DLP) dar. Message Boards, Blogs, Tweets und viele andere Arten von Social Networking bergen Risiken für Information Leakage und Compliance Verletzungen. Die Bedrohungsszenarien für Unternehmen haben dadurch deutlich an Komplexität gewonnen.

IT-SECURITY: EINE BESTANDSAUFNAHME

Angriffe auf die IT: Erfahrungen und Konsequenzen

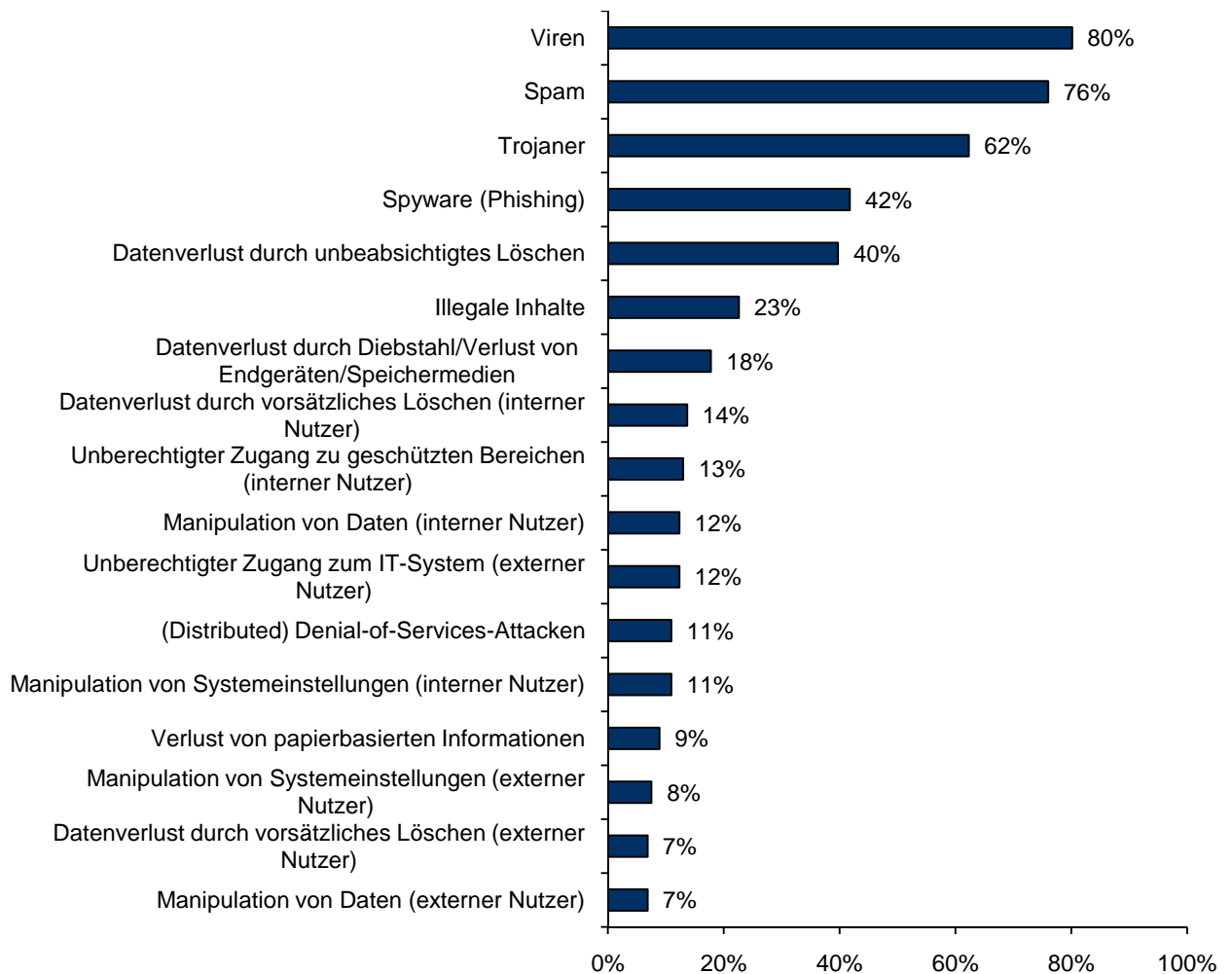
Wie akut und komplex die Bedrohungen auf die Sicherheit der IT sind, zeigt die von IDC im Sommer 2010 durchgeführte Befragung unter 206 Unternehmen in Deutschland mit über 100 Mitarbeitern. Rund drei Viertel der befragten Unternehmen haben bereits bewusst Erfahrungen mit Angriffen auf die Unternehmens-IT gemacht. Es kann zudem davon ausgegangen werden, dass auch die meisten der übrigen Unternehmen Opfer von Angriffen geworden sind, auch wenn sie hiervon keine Kenntnis genommen haben.

Viren, Spam und Trojaner führen die Liste der Angriffe klar an (Abbildung 1). Dies veranschaulicht eindrucksvoll, wie wichtig das Thema Endpoint Security ist, zumal Angriffe dieser Art durch Cyberkriminelle kontinuierlich zunehmen. Daher ist es wenig verwunderlich, dass die Unternehmen beim Einsatz von Security-Lösungen einen starken Fokus auf klassische Endpoint Security Produkte wie beispielsweise Firewalls, Spamfilter oder Antivirus legen.

Stärken Sie das Rechte- und Zugriffsmanagement.

ABBILDUNG 1

Erfahrungen mit Angriffen auf die IT



Quelle: IDC, 2010

Mehrfachantworten möglich

n = 146

Hingegen werden Manipulationen, unberechtigte Zugriffe oder Verluste von Informationen im Vergleich dazu viel seltener bekannt, wenngleich sie ein empfindliches Sicherheitsrisiko für Unternehmen darstellen. Handeln Sie daher verstärkt präventiv und seien Sie sich bewusst über die Risiken solcher Attacken. Legen Sie vor allem ein besonderes Augenmerk auf das Rechte- und Zugriffsmanagement.

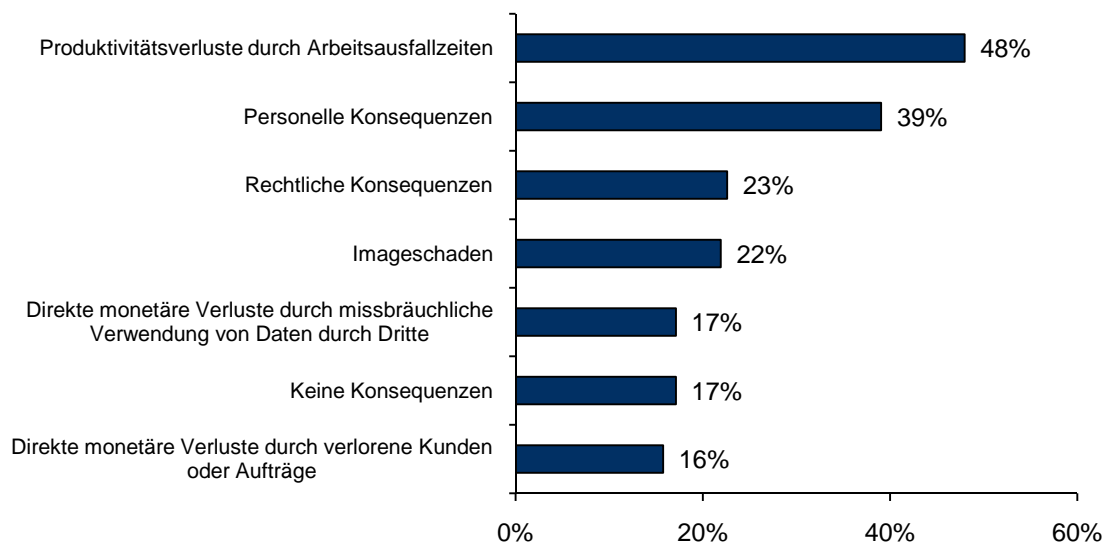
Dass Angriffe auf die IT die Regel und nicht die Ausnahme darstellen, sollte inzwischen jedem IT-Sicherheitsverantwortlichem bewusst sein. Viel wichtiger ist es aber, dass Sie sich im Klaren darüber sind, dass Attacken auf die IT nicht nur das Leben des Sicherheitsverantwortlichen erschweren, sondern auch erhebliche Konsequenzen für das gesamte Unternehmen haben können. Wie die Untersuchung von IDC zeigt, hat fast die Hälfte der Unternehmen mindestens einen Ausfall der IT-Systeme durch Angriffe auf die Unternehmens-IT erlitten, mit der Folge von Produktivitätsverlusten der Mitarbeiter auf der Business-Seite (Abbildung 2). Gerade in Zeiten des steigenden Wettbewerbs- und Preisdrucks ist dies kaum noch hinnehmbar. Außerdem hatten die Angriffe in vielen Unternehmen sowohl personelle als auch rechtliche Konsequenzen. Das wohl wichtigste Gut eines Unternehmens ist aber sein Image. Wird der Ruf eines Unternehmens geschädigt, hat dies meist direkte

Seien Sie sich über die Konsequenzen von Attacken auf die IT für das Unternehmen im klaren, Produktivitätsverluste und Imageschäden müssen vermieden werden.

Auswirkungen auf die Geschäftsentwicklung, wenngleich dieser Schaden am Anfang nur schwer abschätzbar ist. Ein erschreckend hoher Anteil der befragten Unternehmen – immerhin gut 20 % – hat bereits Imageschäden aufgrund von Angriffen auf die IT hinnehmen müssen. Dies veranschaulicht, wie ernst IT Security genommen werden muss. Da außerdem in den vergangenen Monaten eine deutliche Zunahme der Bußgeldverfahren, insbesondere bei Verletzung des Datenschutzes, zu beobachten war und dies aus Sicht von IDC sich auch noch verstärken wird, ist damit zu rechnen, dass vor allem die monetären Verluste weiter steigen werden. Seien Sie sich zudem im Klaren darüber, dass auch die Security-Verantwortlichen zunehmend mit rechtlichen Konsequenzen rechnen müssen.

ABBILDUNG 2

Konsequenzen aus den Angriffen auf die IT



Quelle: IDC, 2010

Mehrfachnennungen möglich

n = 146

Aufgaben und Ausrichtung von IT Security

Primäre und wichtigste Aufgabe der IT-Sicherheit ist nach wie vor die eigentliche aktive Abwehr von Angriffen auf die IT, den Schutz der User und der Daten. Allerdings wird es aus Sicht von IDC immer wichtiger, Präventivmaßnahmen zur Früherkennung von Bedrohungen zu ergreifen. Überdenken Sie ihre IT Security-Strategie. Reagieren Sie lediglich auf akut eingetretene Ereignisse oder sind Sie ihrem "Gegner" einen Schritt voraus? Gehören Sie, wie viele Unternehmen, zur ersten Gruppe, dann ändern Sie ihre Strategie von reaktivem hin zu proaktivem Handeln.

Handeln Sie proaktiv, um so einen kleinen Vorsprung im täglichen Rennen um die IT-Sicherheit Ihres Unternehmens zu gewinnen.

Ganz wichtig für den Erfolg von Sicherheitsmaßnahmen ist zudem eine ganzheitliche Sicht des Themas IT Security, wie es auch im Bundesdatenschutzgesetz (BDSG) gefordert wird. Viele Unternehmen haben bereits ein solches ganzheitliches Sicherheitskonzept eingeführt oder setzen es gerade um. Doch wenn man ehrlich ist, dann ist die Herausforderung nicht ein solches Konzept zu entwickeln, sondern vielmehr, es auch einzuführen und tatsächlich zu leben. Binden Sie unbedingt die Nutzer in Ihrem Unternehmen mit ein, denn der User steht im Zentrum der IT

Security. Mit ihm steht und fällt die erfolgreiche Umsetzung eines jeden Sicherheitskonzepts. Fragen Sie sich immer wieder, ob die User ihr IT Security-Konzept akzeptieren und umsetzen. Ist dies, wie häufig zu beobachten, nicht der Fall, dann suchen Sie nicht die Schuld bei den Anwendern, vielmehr ist das Konzept möglicherweise nicht für ihr Unternehmen geeignet oder die Anwender wurden nicht richtig geschult und aufgeklärt. Meist fehlt den Anwendern einfach nur das Bewusstsein für Sicherheit, was wenig verwundert, denn für sie ist IT nur Mittel zum Zweck. Über Sicherheitsbelange können sie sich im Geschäftsalltag nicht auch noch Gedanken machen und meist wird IT-Sicherheit als lästig empfunden. Daher ist es an Ihnen, die Mitarbeiter entsprechend zu sensibilisieren, sie über Gefahren aufzuklären und insbesondere die Folgen für sie aufzuzeigen, die durch Sicherheitslücken entstehen können. Weisen Sie auf die operativen und strategischen Gefahren für das gesamte Unternehmen hin, dann werden Ihnen Geschäftsführung und Fachbereichsverantwortliche Gehör schenken.

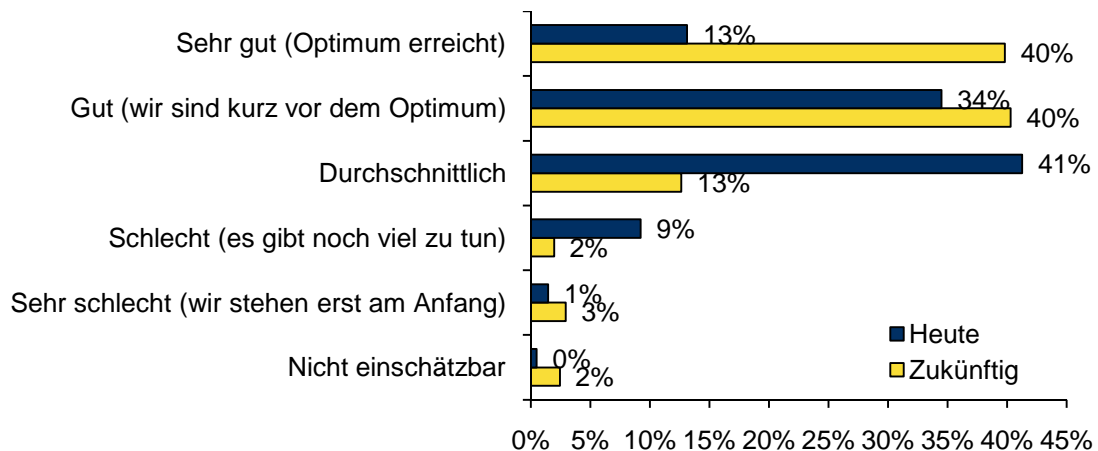
Die User müssen mit ins Boot, sonst sind Sicherheitskonzepte vergeblich.

Beachten Sie in ihrem Sicherheitskonzept auch den Printbereich? Auch Drucker und Multifunktionssysteme stellen potenzielle Sicherheitslücken in der Unternehmens-IT dar. Zu einem ganzheitlichen Ansatz für IT Security gehört daher auch die Integration von Outputgeräten. Viele Unternehmen vernachlässigen diesen Bereich allerdings nach wie vor. Multifunktionssysteme bilden vielfach zentrale Schnittstellen in der Unternehmenskommunikation. Sie bieten nicht nur Funktionen zum Drucken oder Kopieren, sondern können etwa auch E-Mails und Faxnachrichten senden und empfangen. Gescannte Daten können beispielsweise mit einigen Klicks bequem weitergeleitet werden, auch an Adressaten innerhalb und außerhalb des Unternehmens, die diese Informationen nicht erhalten dürften. Mit steigendem Funktionsumfang steigt auch das Risiko, und häufig fehlt hierfür bei den Anwendern schlicht das Risikobewusstsein.

Dass noch erheblicher Handlungsbedarf im Bereich der IT-Sicherheit besteht, verdeutlicht auch die Untersuchung von IDC. Zwar haben relativ viele Unternehmen bereits ein ganzheitliches IT Security Konzept, dennoch stufen viele Sicherheitsverantwortliche die eigene IT Security als nur durchschnittlich ein (Abbildung 3). Nur ein kleiner Teil ist der Meinung, dass sie schon heute das Optimum erreicht hat. Positiv ist, dass die meisten der befragten Unternehmen anstreben, ihre IT Security zu verbessern. In drei bis fünf Jahren will die überwiegende Anzahl der Unternehmen ein gutes bis sehr gutes Level erreicht haben. Das zeigt, dass die meisten Unternehmen erkannt haben, dass sie mehr in IT investieren müssen und verstärkt Maßnahmen zur Verbesserung ihrer IT-Sicherheit ergreifen werden.

ABBILDUNG 3

Einschätzung der eigenen IT Security



Quelle: IDC, 2010

n = 206

Klar ist daher, dass Sie in Ihrem Unternehmen mit steigenden Ausgaben für IT Security rechnen müssen, um Ihre IT wirksam schützen zu können. Planen Sie schon jetzt entsprechende Budgets ein, wenngleich dies in Zeiten eines zunehmenden Kostendrucks schwer zu realisieren sein wird. Setzen Sie daher auf zuverlässige Lösungen, die einfach zu bedienen sind und die vor allem den schnell steigenden Anforderungen sowie der zunehmenden Komplexität der Bedrohungen gerecht werden. Denken Sie zudem über alternative Bezugsmodelle von Sicherheitslösungen nach. Sind Managed Security Services und gehostete Security Services sowie Professional Services in Form von Consulting für Ihr Unternehmen eine kostengünstige und leistungsstarke Alternative, um den zukünftigen Bedrohungspotenzialen begegnen zu können?

Planen Sie steigende Kosten für IT Security ein und denken Sie über alternative Bezugsmodelle aus der Cloud nach.

Virtualisierung und Cloud Computing: Keine Hysterie, aber Gefahren sollten nicht unterschätzt werden

Zwei wesentliche Themen, die IT Security in den nächsten Jahren maßgeblich beeinflussen und verändern, sind Virtualisierung und Cloud Services.

Virtualisierung ist inzwischen bei den meisten Unternehmen Standard. Vor allem bei den größeren Unternehmen, aber auch bei Unternehmen mit sehr komplexen Unternehmensstrukturen ist Virtualisierung weit verbreitet. Am häufigsten wird bisher Server Virtualisierung eingesetzt, aber auch Desktop und Storage Virtualisierung gewinnen zunehmend an Bedeutung.

Die Vorteile, die Virtualisierung mit sich bringt, liegen klar auf der Hand. Die Reduzierung der IT-Kosten und die Möglichkeit, IT flexibler und effizienter einzusetzen haben viele Unternehmen überzeugt, auf Virtualisierung zu setzen. Dennoch sollten Sie die möglichen Risiken der Virtualisierung nicht aus den Augen lassen. So steigt die Anfälligkeit der IT durch eine gestiegene Komplexität der IT-Infrastruktur ebenso wie das Ausfallrisiko. Auch Hypervisorattacken stellen ein potenzielles Risiko dar. Diese Gefahren sollten nicht überbewertet werden und

stehen dem Einsatz von Virtualisierung nicht im Wege, dennoch muss ihnen Beachtung geschenkt werden. Virtualisierung sollte daher nicht ohne definierte Nutzerrichtlinien und Zugangsberechtigungen angewendet werden. Desweiteren wird durch Virtualisierung die Komplexität der Datensicherung erhöht. Dies betrifft auch das Thema Compliance. Zum anderen wird das Management der Sicherheitslücken und der Patch Versionierung komplizierter. Insgesamt ist es daher von höchster Wichtigkeit, bei der Implementierung von Virtualisierung eindeutig festzulegen, wer die Daten besitzt und Zugang erhält. Das gesamte IT Security Management muss mit der Einführung von Virtualisierung strikter werden.

Nutzerrichtlinien und Zugangsberechtigung bei Virtualisierung beachten.

Cloud Computing wiederum ist einer der wichtigsten Trends in der IT-Branche. Schon jetzt nutzt eine Vielzahl von Unternehmen Cloud Services in den unterschiedlichsten Bereichen. Aus Sicht von IDC wird dieser Markt in den kommenden Jahren erheblich wachsen. Dies stellt natürlich auch besondere Anforderungen an das Thema Sicherheit. Vereinbaren Sie insbesondere Service Level Agreements, in dem die Rechte und Pflichten zwischen Ihnen und Ihrem Anbieter eindeutig festgeschrieben sind. Die bisher angebotenen standardisierten Service Level Agreements gehen hier allerdings aus Sicht von IDC oftmals noch nicht weit genug. Auch sollten Sie Themen wie Authentifizierung und Zugriffskontrolle besonders beachten.

Cloud Computing: Beachten Sie in Service Level Agreements auch das Thema Sicherheit.

Regularien und Zertifizierungen

IT-Sicherheit ist aus Sicht von IDC zunehmend eine ganzheitliche Aufgabe. Zwar steht die Technik (die IT) stark im Vordergrund, sie erfordert aber auch organisatorische Maßnahmen wie Unternehmens- und Nutzerrichtlinien sowie Zertifizierungen. Rechtliche Aspekte müssen dabei zwingend eingehalten werden.

Die Untersuchung von IDC zeigt, dass die wichtigsten Richtlinien, die die Security Politik der Unternehmen beeinflussen, interne Sicherheitsrichtlinien und das Bundesdatenschutzgesetz sind (Abbildung 4). Aufgrund seiner Aktualität und seines direkten Bezugs auf die IT hebt sich das BDSG deutlich von den anderen gesetzlichen Vorgaben ab.

Zertifikate, also ein Kennzeichen für quasi "geprüfte Sicherheit", können sowohl gegenüber Ihren Kunden als auch gegenüber Ihren Geschäftspartnern als Qualitätsmerkmal dienen und somit zu einem Wettbewerbsvorteil führen.

Zeigen Sie anhand von Zertifizierungen, dass Sie es mit IT Security ernst meinen.

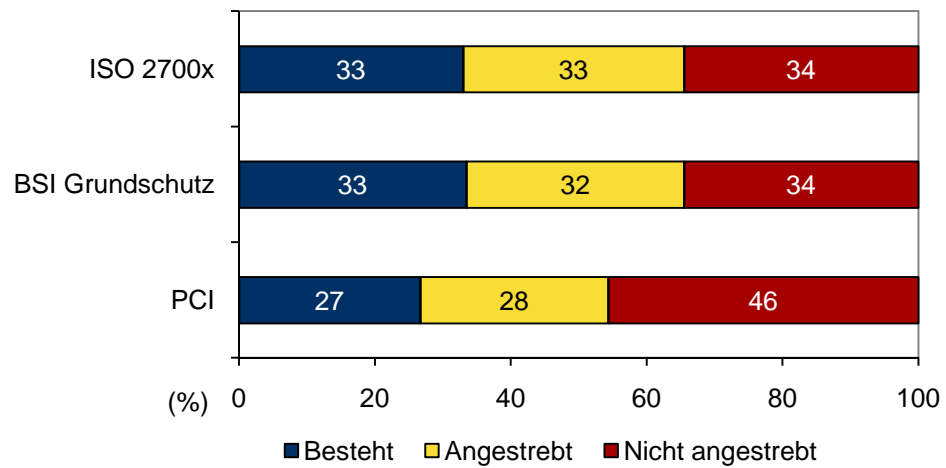
Anerkannte Standards sind vor allem die internationale Norm ISO 2700x, welche die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten Informationssicherheits-Managementsystems unter Berücksichtigung der Risiken innerhalb der gesamten Organisation spezifiziert. Diese Norm ist ein hilfreicher Standard für Ihre IT-Sicherheit und immer mehr Unternehmen streben diese Zertifizierung an (Abbildung 5).

Ganz ähnlich verhält es sich mit dem nationalen (deutschen) IT Grundschutz. Das BSI unterteilt die Gefahren in organisatorische Mängel, menschliche Fehlhandlungen, technisches Versagen und vorsätzliche Handlungen. Zu ersterem gehören etwa Fehler bei der Planung. IT-Grundschutz bietet eine einfache Methode, dem Stand der Technik entsprechende Sicherheitsmaßnahmen zu identifizieren und umzusetzen. Das BSI stellt zahlreiche Werkzeuge zur Verfügung, um ein angemessenes Sicherheitsniveau zu erreichen, wie z.B. die BSI-Standards zum Informationssicherheitsmanagement, die IT-Grundschutz-Kataloge und das GSTOOL. Erst

kürzlich hat das BSI auf die steigende Verbreitung von Virtualisierung reagiert und einen Entwurf für einen weiteren Baustein hierzu vorgelegt. Der BSI Grundschutz stellt damit eine gute Methode zur Grundabsicherung Ihres Unternehmens dar.

ABBILDUNG 4

Verbreitung von Zertifizierungen



Quelle: IDC, 2010

Abweichung von 100% durch Rundung

n = 206

EMPFEHLUNGEN

IDC Empfehlungen

Auf Basis der Befragungsergebnisse leitet IDC verschiedene Empfehlungen für Unternehmen ab:

Ganzheitlicher Ansatz

Die Vielschichtigkeit und Variantenvielfalt der möglichen Angriffe auf die IT-Sicherheit eines Unternehmens erfordert eine ganzheitliche Betrachtung des Themas IT Security. Dabei müssen insbesondere die individuellen Gefahrenpotenziale der Unternehmen einfließen. Dies bedeutet, dass Sie die Bedrohungslage Ihres Unternehmens insgesamt erfassen und einzelne Sicherheitskomponenten und –maßnahmen in eine Gesamtlösung zusammenführen müssen.

Verfolgen Sie ein ganzheitliches Konzept und führen Sie integrierte Produkte anstelle von Einzellösungen ein. Wichtig ist eine klare Formulierung der Ziele der Sicherheitslösungen und die objektive Bestimmung der Sicherheitsanforderungen. Zudem sollten Sie einen effektiven Prozess zur Gewährleistung der IT-Sicherheit etablieren. Dabei muss klar sein, dass IT-Sicherheit kein Projekt mit einem Anfang und einem Ende ist.

Mitarbeiter sensibilisieren

Die meisten Sicherheitsrisiken entstehen durch die Anwender innerhalb eines Unternehmens. Oftmals wird IT Security nur als lästige Pflicht wahrgenommen, die ein effektives Arbeiten erschwert. Sicherheitsmaßnahmen können aber nur greifen, wenn die Sicherheitskonzepte auch gelebt werden. Sicherheitsrichtlinien und eine Sensibilisierung der Mitarbeiter sind daher unumgänglich, um einen wirksamen Schutz des Unternehmens zu gewährleisten.

Stärkeren Sie daher das Bewusstsein bei den Anwendern und vor allem bei der Unternehmensführung für die Bedrohungspotenziale und schärfen Sie das Verständnis für Veränderungen der Gefahrenlage und neue Lösungsansätze. Hier sollten Sie speziell auf die betriebswirtschaftlichen und rechtlichen Konsequenzen hinweisen, verzichten Sie aber auf überzogene Schreckensszenarien.

Cloud Computing beachten

Cloud Computing ist einer der wichtigsten Trends in der IT-Branche. Schon jetzt nutzt eine Vielzahl von Unternehmen Cloud Services in den unterschiedlichsten Bereichen. Aus Sicht von IDC wird dieser Markt in den kommenden Jahren erheblich wachsen. Evaluieren Sie, ob Cloud-basierte Managed Security Services wie z.B. Denial-of-Service Defense, Netzwerk, Messaging oder Web Security für Ihr Unternehmen eine attraktive Alternative gegenüber herkömmlichen Bezugsmodellen von Sicherheitslösungen darstellt.

Sicheres Drucken vorantreiben

Ein nach Meinung von IDC derzeit noch stark unterschätztes Thema betrifft "sicheres Drucken". Allerdings zeigen die Befragungsergebnisse, dass sich immer mehr Unternehmen darüber im Klaren sind, dass auch dieser Bereich gesichert werden muss. Gleichzeitig wird Drucken von vielen Unternehmen aber nach wie vor nicht als Bereich gesehen, den es zu schützen gilt. Seien Sie sich der Risiken und Folgen im

Druckbereich bewusst. Schaffen Sie ein Risikobewusstsein bei den Usern und klären Sie sie über entsprechende Gefahren auf.

Compliance und Zertifizierung

Immer wichtiger wird die Einhaltung von rechtlichen Vorschriften. In Zukunft wird dieses Thema aus Sicht von IDC weiter an Bedeutung gewinnen, neue gesetzliche Vorschriften, eine verschärfte Verfolgung von Verstößen, aber auch interne Regeln erschweren das Thema Compliance. Scheuen Sie sich nicht, hierbei auf externe Hilfe zurückzugreifen.

Zeigen Sie Ihren Kunden und Geschäftspartnern durch Zertifizierungen, wie z.B. ISO 2700x, dass Sie es in Ihrem Unternehmen mit dem Thema IT Security ernst nehmen.

Empfehlungen von Anwendern für Anwender

Nachfolgend sind einige Empfehlungen dargestellt, die die befragten Anwender anderen Unternehmen mit auf den Weg geben wollten:

- "Beachten aller möglichen Risiken, proaktives Handeln und manchmal auch etwas tiefer in den Geldbeutel greifen, um eine saubere Lösung zu erhalten."
- "Das Bestmögliche herausholen, auch wenn es etwas mehr Geld kostet. Der Imageschaden wäre andererseits immer höher als die Ausgaben."
- "Man sollte sich im Bereich Security auf alle Fälle externe, fachliche Hilfe nehmen, da es sich bei Security-Themen um sehr unternehmensbrisantere Themen handelt, die nicht mit einem Halbwissen bearbeitet werden sollten!"
- "Der Anfang ist immer schwer. Hilfreich ist ein IT-Sicherheitsbeauftragter, der auch einmal unpopuläre Dinge durchsetzt und sich nicht immer "auf der Nase rumtanzen" lässt."
- "Der Mensch ist in der Regel die größte Schwachstelle. Zu komplexe und nutzerunfreundliche Systeme erhöhen weniger die Sicherheit, sondern führen bei den Mitarbeitern eher zu "nutzerfreundlichen", teilweise hochgradig unsicheren 'Eigenlösungen'."
- "Die Mitarbeiter müssen ausreichend hinsichtlich der IT-Risiken aufgeklärt/sensibilisiert werden. Sonst nützt die beste Konzeption nichts."
- "Es ist definitiv auf Dauer günstiger, mit renommierten Anbietern zusammenzuarbeiten und umfassende Lösungen sofort anzustreben, als etappenweise vorzugehen und dabei Trial and Error mit Billiganbietern zu erleben."
- "Gute Mischung aus Sicherheit und Praktikabilität erarbeiten. Gesamtpaket in mehrere kleinere packen, so lässt es sich besser umsetzen und die Akzeptanz ist größer."
- "Man wird erst aus Schaden klug."

METHODIK

Bei dem vorliegenden Dokument handelt es sich um einen Auszug aus der Multi-Client-Studie "IT-Security – Trends und Anwenderpräferenzen, Deutschland 2010 ", die u.a. von Kaspersky Lab gesponsert wurde.

Von Mai bis Juni 2010 befragte IDC 206 Unternehmen in Deutschland aller Größenklassen und Branchen mit mehr als 100 Mitarbeitern zum Thema IT Security. Es wurden hauptsächlich Fach- und Führungskräfte aus dem IT-Abteilungen befragt, in deren Verantwortungsbereich Security fällt.

Die Darstellung des Unternehmensprofils sowie der Fallstudie von Kaspersky Lab basieren auf Informationen, die von Kaspersky Lab zur Verfügung gestellt wurden. Für diese Angaben übernimmt IDC keine Gewähr.

ANHANG

Unternehmensdarstellung Kaspersky Labs GmbH

Informationen zum Unternehmen

Das Unternehmen Kaspersky Lab ist auf Produkte und Services für die IT-Sicherheit spezialisiert. Der global agierende Software-Entwickler mit Hauptsitz in Moskau bietet Security-Lösungen an, um IT-Bedrohungen wie Viren, Spyware, Trojaner, Hacker, Phishing-Attacken und Spam abzuwehren.

Kaspersky Lab beschäftigt weltweit über 1.700 Mitarbeiter, deren Know-how sich in der Qualität der Produkte widerspiegelt. Im Unternehmen arbeiten spezialisierte Mitarbeiter, darunter Mitglieder der Computer Anti-Virus Research Organization (CARO), zudem bestehen Partnerschaften mit bedeutenden IT-Herstellern. IDC listet Kaspersky Lab in seinem „Worldwide Software 2009-2013 Forecast Summary“ unter den weltweiten Top 100 der Anbieter von Anwendungssoftware, nach Umsätzen im Jahr 2008.

Sowohl die deutsche Niederlassung als auch die Europa-Zentrale befinden sich in Ingolstadt. Dort sind rund 140 Mitarbeiter tätig, die sich um das Marketing, den Vertrieb und den Support kümmern.

Positionierung im Bereich IT Security

Die Palette der angebotenen Produkte reicht von Antiviren-Software bis hin zum Komplettschutz mit Firewall, Spam-Filter und weiteren Sicherheitstools. Dabei gibt es für alle Zielgruppen vom Heimanwender über kleine und mittlere Unternehmen bis hin zu großen Firmen speziell zugeschnittene Angebote. Über die eigenen Produkte hinaus ist Kaspersky-Technologie auch Bestandteil vieler Produkte und Dienstleistungen führender IT-Sicherheitsanbieter.

Darstellung des IT Security Portfolios

Produkte für Heimanwender

Für Heimanwender hat Kaspersky Lab etwa die Produkte Kaspersky PURE, Kaspersky Internet Security 2011 und Kaspersky Anti-Virus 2011 im Programm und bietet hiermit ein umfassendes Portfolio für private Nutzer. Daneben bietet Kaspersky Lab mit Kaspersky Mobile Security auch eine Lösung für Smartphones unter Symbian oder Windows Mobile. Für den Virenschutz von Apple-Rechnern ist Kaspersky Anti-Virus for Mac im Sortiment.

Produkte für Unternehmen

Die Komplettpakete der Unternehmenslösung Kaspersky Open Space Security sorgen in vier Ausbaustufen für den Schutz von Workstations, Datei-Servern, Mail-Server und Internet-Gateways sowie von mobilen Geräten. Mit dem Kaspersky Administration Kit ist eine zentrale Installation und Steuerung aller installierten

Komponenten auch in heterogenen Netzwerken möglich. Neben Windows- und Linux-Plattformen – unterstützt werden alle bekannten Linux-Distributionen und FreeBSD – sollten Kaspersky-Produkte auch Server unter Novell Netware sowie Citrix-Terminal-Server schützen.

Speziell für den SMB-Bereich bietet Kaspersky Lab das 5+1 Base Pack mit Lizenzen zum Schutz eines Datei-Servers und bis zu fünf Workstations an. Über Expansion Packs kann dieser Schutz um weitere Workstations erweitert werden. So können auch kleine Firmen ihr Netzwerk laut Hersteller einfach und kostengünstig absichern, bei Bedarf wächst der Virenschutz dann mit der steigenden Mitarbeiterzahl mit.

Referenzen im Bereich IT Security (in Deutschland)

- ☒ XXXLutz KG
- ☒ s.Oliver GmbH
- ☒ Malteser Hilfsdienst gGmbH

Fallstudie: s.Oliver

Informationen zum Kunden

Der Name s.Oliver lässt es kaum vermuten, dennoch hat das 1969 von Bernd Freier gegründete Modeunternehmen auch heute noch seinen Sitz im Fränkischen Rottendorf.

Anforderungen des Kunden

Rund 5.500 Mitarbeiter sind heute für das Mode- und Lifestyle-Unternehmen weltweit tätig, s.Oliver-Produkte sind in über 30 Ländern zu finden. Als Folge der Expansion entstand ein weit verzweigtes Unternehmensnetzwerk, in dem Kommunikation und vor allem E-Mail-Korrespondenz eine entscheidende Rolle spielt. Den elektronischen Nachrichtenfluss zu sichern, ist daher essentiell für das Modeunternehmen. Seit 2009 baut s.Oliver hierbei auf Kaspersky Lab.

Darstellung der Lösung

Michael Muthig, Head of IT-Services bei s.Oliver, weiß, wie wichtig eine adäquate Sicherheitslösung vor allem zum Schutz der Unternehmens-Mails ist: „Bevor wir auf Kaspersky Lab setzten, wurden unsere E-Mails von lediglich einem Antiviren-Programm gescannt. Um unser Unternehmen möglichst umfassend zu schützen, lassen wir unseren E-Mail-Traffic mittlerweile von zwei Lösungen überwachen. Kaspersky Lab komplettiert also unsere IT-Infrastruktur und sorgt für einen sicheren elektronischen Nachrichtenfluss bei s.Oliver.“

Damit IT-Gefahren erst gar nicht in das Unternehmensnetzwerk eindringen, entschieden sich die IT-Verantwortlichen bei s.Oliver für Kaspersky Security für Mail

Server. „Mit der Kaspersky-Lösung werden alle unsere eingehenden E-Mails effektiv bearbeitet. Der Gateway-Schutz minimiert das gesamte Viren- und Spam-Aufkommen in unserem E-Mail-Verkehr. Finanzielle Einbußen, verursacht durch Viren, Würmer und Co, blieben uns so in den vergangenen Jahren erspart“, zeigt sich Thomas Steinhart, Chief Financial Officer bei s.Oliver, erfreut.

Die IT-Infrastruktur bei s.Oliver ist auf VMWare vSphere 4 sowie SUSE Linux 10 aufgebaut. Die Entscheidung für Kaspersky Security für Mail Server – mit derzeit 3.500 eingesetzten Lizenzen – lag nahe, da die Lösung auch Linux-Mailserver absichert. Die Integration der Kaspersky Anti-Spam Engine 3.0 bietet den IT-Administratoren bei s.Oliver zudem ein neues System zur Analyse der Betreffzeilen von E-Mails und grafischen Anhängen sowie die Nutzung des Urgent Detection System (UDS), das in Echtzeit auf den Erhalt von Spam reagiert.

Michael Muthig zieht ein durchwegs positives Fazit, wenn er die Kooperation mit Kaspersky Lab Revue passieren lässt: „Gleich nachdem die Kaspersky-Software implementiert war, lief sie sehr sicher und stabil. Neben der leichten Administrierbarkeit einer der Gründe, warum wir mit der Lösung von Kaspersky Lab sehr zufrieden sind“.

Projekthighlights

- ☒ IT-Infrastruktur des Kunden aufgebaut auf VMWare und SUSE
- ☒ 3.500 eingesetzte Kaspersky Security for Mail Server Lizenzen
- ☒ 4 Jahre Laufzeit
- ☒ 2009 Erweiterung um 500 Lizenzen auf 3.500 Lizenzen

Copyright Hinweis

Die externe Veröffentlichung von IDC Information und Daten – dies umfasst alle IDC Daten und Aussagen, die für Werbezwecke, Presseerklärungen oder anderweitige Publikation verwendet werden, setzt eine schriftliche Genehmigung des zuständigen IDC Vice Presidents oder des jeweiligen Country-Managers bzw. Geschäftsführers voraus. Ein Entwurf des zu veröffentlichenden Textes muss der Anfrage beigelegt werden. IDC behält sich das Recht vor, eine externe Veröffentlichung der Daten abzulehnen.

Für weitere Informationen bezüglich dieser Veröffentlichung kontaktieren Sie bitte: Katja Schmalen, Marketing Manager, +49 (0)69/905020 oder kschmalen@idc.com.

Urheberrecht: IDC, 2010. Die Vervielfältigung dieses Dokuments ist ohne schriftliche Erlaubnis strengstens untersagt.