

IDC Executive Brief

IT Security in Deutschland 2011

Neue Herausforderungen durch Cloud Computing, Mobilität und Social Media

.....
Gesponsert von Siemens Enterprise Communications
.....

INHALTSVERZEICHNIS

	S.
Einleitung	1
Trends und Entwicklungen in Deutschland	1
IDC Empfehlungen	7
Empfehlungen von Anwendern für Anwender	8
Methodik	9
Siemens Enterprise Communications	10
Fallstudie: Sportcast GmbH.....	10

ABBILDUNGSVERZEICHNIS

	S.
1 Top-Herausforderungen für die IT-Sicherheit.....	2
2 Sicherheitslevel - Selbsteinschätzung.....	4

EINLEITUNG

IT Security genießt in den IT-Abteilungen deutscher Unternehmen hohe Priorität. Seit Jahren steht die Absicherung der eigenen Informationstechnologie und der IT-Landschaft vor Bedrohungen weit oben auf der Agenda von IT-Verantwortlichen.

Allerdings gibt es keine absolute Sicherheit. IT Security wird immer komplexer und aufwendiger und hat regelmäßig neue Facetten. Die Unternehmens-IT ist eine zunehmend offene Landschaft, in der einerseits bestimmte Grenzen scharf gezeichnet sind und andererseits immer wieder neue Schlupflöcher entstehen, Lücken sichtbar werden und Anwendungen zu neuen Lösungen zusammengefügt werden. Cloud Services, mobile Endgeräte oder Web 2.0 Technologien stehen für diese Grenzaufweichung und die kontinuierlichen Veränderungen.

Jedes Unternehmen hat spezifische und individuelle Sicherheitsanforderungen. Die IT muss diesen Anforderungen Rechnung tragen und individuelle Gefährdungspotenziale kontinuierlich analysieren. Die Bedrohungsszenarien wandeln sich permanent. Sie werden granularer. Ihre Zahl steigt. Alle Trends in der IT werden stets auch auf ihr Schadpotenzial in "abgeklopft".

TRENDS UND ENTWICKLUNGEN IN DEUTSCHLAND

IT-Sicherheit im Fokus

IDC hat im Juni 2011 202 Unternehmen mit mehr als 100 Mitarbeitern befragt, um ein besseres Verständnis für den Umgang der Firmen mit IT-Sicherheitslösungen und Reaktionen auf Bedrohungsszenarien zu erhalten und die sich wandelnden sicherheitsrelevanten Fragestellungen der Anwender zu verstehen.

Das vorliegende Dokument fasst die wichtigsten Ergebnisse dieser Befragung für IT Security-Verantwortliche in Unternehmen zusammen.

Herausforderungen für die IT-Sicherheit

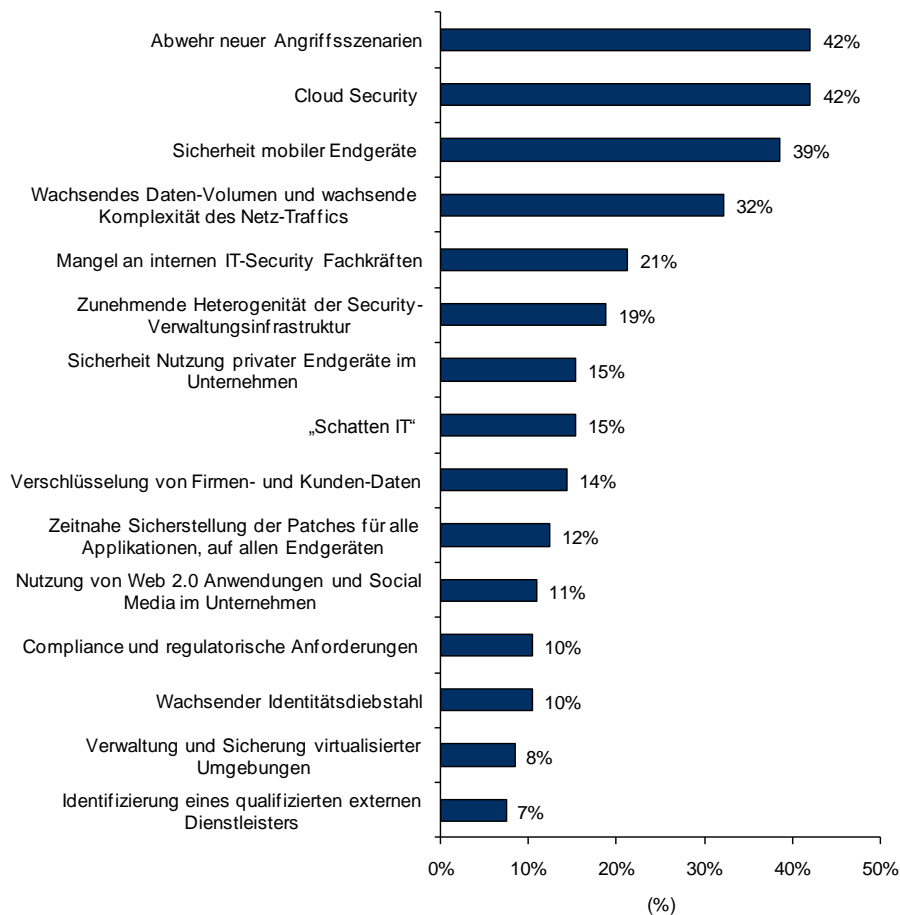
Eine hohe IT-Sicherheit kann nur dann erreicht werden, wenn Sie sich über die wesentlichen Herausforderungen im Klaren sind. Gefährdungen für Unternehmen können aus vielfältigen Ursachen entstehen. Gefahrenquellen liegen im Wesentlichen in Programmierfehlern, Konzeptionsfehlern, Konfigurationsfehlern und menschlichem Fehlverhalten. Im Falle von Programmierfehlern benötigen die Unternehmen Hilfe beim Erkennen der Fehler und beim Patchen der Lücken. Konzeptionsfehler und Konfigurationsfehler sind echte Gefährdungsquellen, deren Vermeidung oder Verringerung spezielles Know-how erfordert.

Aus den zahlreichen Herausforderungen haben sich im Rahmen der Befragung aber einige Themen herauskristallisiert. 42 % der befragten Unternehmen betrachten die Abwehr neuer Angriffsszenarien als wichtigste Herausforderung. Dieser Wert drückt ein Stück weit Unsicherheit aus. Unternehmen wissen zwar, dass in vielen Anwendungen Fehler und Lücken verborgen sind, aber sie können nur schwer abschätzen, welches Risiko dies für ihr eigenes Unternehmen bedeutet. Zu weiteren Top-Herausforderungen der Firmen zählen Cloud Security (42 %) und die Sicherheit mobiler Endgeräte (39 %). Beide Themen fallen unter dem Gesichtspunkt IT-Sicherheit ebenfalls unter die eher neueren Fragestellungen. Während Cloud Services derzeit lediglich für einen Teil der Unternehmen von Relevanz sind, müssen

sich immer mehr Unternehmen mit der Sicherheit von mobilen Endgeräten und "mobilen" Geschäftsprozessen auseinandersetzen.

ABBILDUNG 1

Top-Herausforderungen für die IT-Sicherheit



Quelle: IDC, 2011

Mehrfachnennungen möglich

n=202

Unternehmen sehen sich mit wachsendem Datentransfer und unterschiedlichen Datenquellen konfrontiert. Eine zunehmende Heterogenität betrifft nicht nur die Daten selbst, sondern auch die Art und Weise, wie sie gespeichert, verwaltet, bearbeitet und weitergegeben werden. In einigen Unternehmen hat sich beispielsweise eine sogenannte Schatten-IT entwickelt. Solche Systeme, die außerhalb der Verantwortung der zentralen IT-Organisation laufen, müssen ebenfalls hinsichtlich IT-sicherheitsrelevanter Aspekte betrachtet werden. Im schlimmsten Falle sind den zentralen IT-Stellen solche Systeme oder Veränderungen an den Systemen nicht bekannt; eine große potenzielle Gefahrenquelle für das Unternehmen im Ganzen.

Gefährdungsfaktor Mitarbeiter

Die Hälfte der im Rahmen der Studie befragten Unternehmen benannte die Mitarbeiter als schwächstes Glied ihrer IT Security-Kette, gefolgt von Smartphones, Laptops und PC-Arbeitsplätzen.

IT Security wird in vielen Unternehmen noch nicht hinreichend ernst genommen. An erster Stelle bei den internen Bedrohungs- und Risikopotenzialen wird das mangelnde Sicherheitsbewusstsein der Mitarbeiter genannt. Das reicht von Ignoranz über Ausblenden von Risiken bis hin zu Unwissenheit. Aber auch ein vorsätzliches Fehlverhalten wird als mögliche Gefahrenquelle in Erwägung gezogen. Vielfach gelingt es IT- und Security-Verantwortlichen nur schwer, den Entscheidern die Risiken und die damit einhergehenden Konsequenzen deutlich zu machen. Sicherheit wird zu oft auch noch als lästiges IT-Thema verstanden. Hier müssen Unternehmen mehr Aufklärungsarbeit leisten und auch auf die mit IT Security Risiken zusammenhängenden operationalen und strategischen Risiken hinweisen. Sichern Sie sich die Unterstützung der Unternehmensführung und der Fachverantwortlichen zur Stärkung der IT-Sicherheit in Ihrem Unternehmen.

Die Frage ist nicht ob, sondern wann Ihr Unternehmen angegriffen wird

Angriffe oder Kompromittierungsversuche werden entweder gezielt oder zufällig vorgetragen. Aktuell stellt sich die Frage nicht, ob ein Unternehmen attackiert worden ist, sondern wann es angegriffen wurde und ob der Angriff erfolgreich war. 21 % der befragten Unternehmen gesteht ein, bereits Opfer erfolgreicher Angriffe geworden zu sein. 7 % können dies nicht mit Sicherheit sagen und 72 % der Unternehmen glauben, bisher von Angriffen verschont worden zu sein. Es kann aber davon ausgegangen werden, dass auch die meisten Unternehmen zumindest attackiert worden sind oder, dass sie Opfer von Angriffen wurden, ohne dass sie davon Kenntnis genommen haben.

Die Motivationen der Angreifer und die Wahl der technischen Mittel unterscheiden sich. Spyware, Malware und ein unberechtigter Zugang zum IT-System führen die Liste der Art der Angriffe an. Diese Angriffe zielten entweder auf das Unternehmen in seiner Gesamtheit oder auf einzelne Unternehmensbereiche, wie etwa den Vertrieb mit seinen Kundendaten oder den Finanzbereich mit entsprechenden Finanzdaten ab.

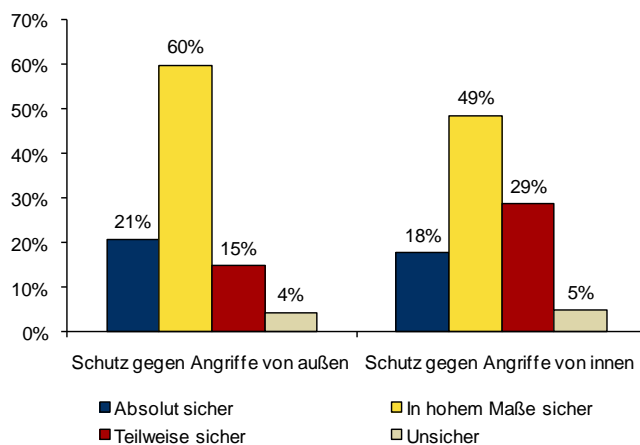
Mehr als 20 Prozent der Unternehmen fühlen sich absolut sicher

Nichtsdestoweniger geben sich befragten Unternehmen hinsichtlich der Qualität ihrer Schutzvorkehrungen und Schutzeinrichtungen durchaus überzeugt.

21 % der befragten Unternehmen stufen den Schutz gegen Angriffe von außen als absolut sicher und 60 % als in hohem Maße sicher ein. 15 % der Unternehmen attestieren sich eine teilweise Sicherheit, 4 % der Befragten schätzen den Schutz gegen Angriffe von außen als unsicher ein. Den Schutz gegen Angriffe von innen, also innerhalb der Unternehmensgrenzen werten die Befragten kritischer. Der Anteil der Nennungen für eine absolute Sicherheit liegt hier bei 18 %, 49 % der Befragten sind der Meinung, sie seien in hohem Maße sicher. 29 % gehen von einer teilweisen Sicherheit aus, 5 % schätzen die Situation als unsicher ein. Wo sehen Sie Ihr Unternehmen heute? Wo wird es morgen stehen? Viele Sicherheitsverantwortliche sind sich der Tatsache bewusst, dass das Halten eines hohen Sicherheitsstandards permanent Ressourcen erfordert.

ABBILDUNG 2

Sicherheitslevel - Selbsteinschätzung



Quelle: IDC, 2011

n=202

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. Reagieren Sie lediglich auf akut eingetretene Ereignisse oder sind Sie ihrem "Gegner" einen Schritt voraus? Gehören Sie, wie viele Unternehmen, zur erstgenannten Gruppe, dann ändern Sie ihre Strategie von reaktivem hin zu proaktivem Handeln.

Unternehmen investieren künftig in Data Leakage/Loss Prevention , PKI und Intrusion Detection/Intrusion Prevention

In den vergangenen Jahren haben Firmen intensiv in Sicherheitsprodukte und -lösungen investiert. Die befragten Unternehmen sind in hohem Maße mit IT Security Lösungen und Produkten ausgestattet. Solche Basistools wie Firewalls, Antivirus-Schutz und Spamfilter sind flächendeckend im Einsatz oder Bestandteil von Planungen.

IDC geht von steigenden Anforderungen an Endpoint Security aus, um Unternehmensinformationen und Daten vor unerlaubtem Zugriff zu schützen. In Summe werden Endpoint Security Lösungen durch die sich ständig verändernden Bedrohungen noch lange nicht Commodity werden. Unternehmen und Organisationen müssen sich in Zukunft immer mehr Gedanken um ihre Sicherheit machen und sich spezifisch mit ihren eigenen Sicherheitsrisiken beschäftigen. Hier bietet sich ein guter Ansatzpunkt für Anbieter von IT Security Services.

Bei den Planungen der befragten Unternehmen zu verschiedenen Lösungen wurden folgende Themen am häufigsten genannt: Data Leakage/Loss Prevention (48 %), PKI (43 %), Intrusion Detection/Intrusion Prevention (41 %), Biometrische Verfahren (41 %) und Schwachstellenmanagement (41 %).

Mit der Vielfalt der eingesetzten Sicherheitslösungen benötigen Unternehmen eine Gesamtsicht auf ihre IT Security. So muss beispielsweise sichergestellt sein, dass alle genutzten IT-Sicherheits-Tools optimal aufeinander abgestimmt sind und sich gegenseitig nicht negativ beeinflussen. Punktlösungen sollten möglichst vermieden

werden und Ausgaben immer im Sinne einer übergreifenden Sicherheitsstrategie getätigt werden.

IT-Security Budgets wachsen

In den meisten deutschen Unternehmen wachsen die Budgets für IT Security in den kommenden Jahren. Viele Unternehmen erkannt haben, dass sie kontinuierlich in die IT-Sicherheit investieren müssen und erhöhen die Ausgaben zur Verbesserung ihrer IT Security. Mehr als zwei Drittel der Befragten planen steigende Ausgaben für IT Security in den nächsten zwei Jahren. Immerhin 35 % der Befragten rechnen hier mit einem Ausgabenwachstum von mehr als 10 %. Ca. 18 % rechnen mit einem gleichbleibenden Investitionsvolumen und lediglich 3 % erwarten sinkende Ausgaben. Somit verfügen Sie über gute Argumente, um auch für Ihr Unternehmen höhere IT-Sicherheitsbudgets einzuwerben.

IT-Sicherheit für neue Themen und Technologien

Cloud Services: Chancen für höhere IT-Sicherheit

IT-Sicherheit kann im Kontext Cloud Computing unterschiedliche Ausprägungen haben. IDC unterscheidet zwischen Security aus der Cloud in Form von Security-as-a-Service und der sicheren Nutzung von Cloud Services.

Security-as-a-Service als Bereitstellungsform von externen IT Security Services aus der Cloud stellt für zirka ein Drittel der Unternehmen eine interessante Option dar. Mittelständische sollten nach Ansicht von IDC den Wert von Security-as-a-Service für ihr Unternehmen prüfen. Aus Sicht der Unternehmen sprechen kurze Reaktionszeiten auf Veränderungsanforderungen (Signatures, Files, Update und Code Fixes), geringe Bereitstellungs- und Nutzungskosten sowie eine zentrale Verwaltung der Ereignisdokumentation für Security-as-a-Service. Security-as-a-Service und Cloud-basierte Managed Security Services, wie z.B. Denial-of-Service Defense, Netzwerksicherheit, Messaging oder Web Security, werden zunehmend von einigen Providern angeboten.

Cloud Services in Deutschland werden in steigendem Maße angenommen und der Markt gewinnt langsam an Reife. Hieraus ergeben sich neue Anforderungen für die IT-Sicherheit, unabhängig davon, ob es sich um Public, Private oder Hybrid Cloud-Szenarien handelt. Unternehmen müssen das Thema Cloud Services sehr sorgfältig angehen und dem Thema IT-Sicherheit einen großen Stellenwert einräumen. Um Risiken beim Bezug von Cloud Services zu vermeiden beziehungsweise abzuwehren und eine höhere Datensicherheit zu erreichen sind Aktivitäten bereits im Vorfeld notwendig. So führen 54 % der befragten Unternehmen beispielsweise eine Optimierung der internen IT Security im Vorfeld und 41 % IT Security Assessments der internen IT durch. Prüfen Sie, welche Sicherheitsstandards Ihr Provider bietet. Anbieter vom Cloud Services sollten zumindest ein Information Security Management System auf Basis der gängigen Standards (IT-Grundschutz, ISO 2700x, etc.) implementiert haben.

Mobile Security hat viele Facetten

Mobile Security wird für Unternehmen immer wichtiger, da mobile Plattformen und Anwendungen in den letzten Jahren stetig zugenommen haben und die meisten Geschäftsprozesse eine oder mehrere mobile Komponenten besitzen. Lässt man die Kategorie Notebooks/Laptops unberücksichtigt, ist davon auszugehen, dass die reine Anzahl der Bedrohungspotenziale im mobilen Umfeld bisher noch geringer ist als in der IT allgemein. Durch die Anbindung an unternehmensweite Netzwerke ist aber

bereits eine kritische Stufe erreicht und IDC rechnet damit, dass sich dies zunehmend verstärken wird.

Ist Ihnen das Risikopotenzial mobiler Lösungen bekannt? Am häufigsten (jeweils 2,6) wurden in der Befragung die Nutzung nicht autorisierter bzw. nicht lizenzierter Programme, Datenverlust und die Nutzung von Apps genannt. Die weiteren Nennungen waren Einfalltor für Schadcode: 2,7; Nutzung von Social Media: 2,7; Identitätsdiebstahl: 2,7; geringe Verlusthürde: 2,8 sowie Rufschädigung: 3,0. Die Risiken sind in der Tat hoch.

Über nicht autorisierte Programme kann Schadcode eingeschleust werden, da solche Programme mitunter von fragwürdigen Quellen bezogen werden. Zudem ist das ein Verstoß gegen die Nutzungsbedingungen des Softwareproduzenten. Häufig werden Attacken über Social Networking-Seiten initiiert. Die Angreifer nutzen dann auch Schwachstellen der Endgeräte aus.

Die auf mobilen Devices gespeicherten Businessdaten und Verbindungsdaten werden für Hacker zunehmend interessant, was eine zunehmende Zahl von Viren, Malware und Exploits nach sich zieht. IDC erwartet, dass im Jahr 2015 Lösungen für Mobile Threat Management (Antimalware, Firewall, IDS, Antispam) den größten Anteil im Markt für mobile Security Lösungen ausmachen werden.

Die befragten Unternehmen setzen Mobile Security Software für unterschiedliche Einsatzszenarien ein. Am häufigsten wird die Nutzung von Mobile Secure Content Management und Threat Management (MSCTN) genannt. MSCTN führt die Liste der Häufigkeit der Nennungen (47 %) an, Mobile VPN folgt mit 43 %. Mobile IPC verzeichnet 28 % der Nennungen. Auch Sicht von IDC sollten Anwender auf eine einfache Implementierung und Installation von Mobile Security Software achten. Der komfortabelste Weg ist der über die Mobilfunkverbindung selbst. Neben rein technischen Aspekten können die Konvergenz von Telekommunikation und IT, Compliance oder Social Networks das Einführen von Mobile Security Software anstoßen.

Social Media und Web 2.0 erfordern Security-Konzepte

Social Media-Anwendungen und Web 2.0 Tools haben Einzug in zahlreiche Unternehmen gehalten. Facebook, Twitter, LinkedIn oder ähnliche Tools bieten sehr gute Kommunikationsmöglichkeiten. Ihre Nutzung ist aber nicht gefahrlos. In Social Media-Anwendungen werden auch falsche Identitäten genutzt und Malware verbreitet. Nutzt Ihr Unternehmen lediglich firmeneigene Accounts und Tools oder setzen Anwender mitunter auch private Accounts für berufliche Zwecke ein? Verfügen Sie über einen vollständigen Überblick über die Aktivitäten in diesem Umfeld? Ist klar geregelt, wer welche Tools wie nutzen darf? Sind die Verantwortlichkeiten zwischen der IT und den Fachbereichen geklärt? Ist den Anwendern bewusst, welche Gefahren sich hier verbergen können?

Laut Befragung haben heute z.B. 34 % der Unternehmen beispielsweise Richtlinien zur sicheren Nutzung unternehmenseigener Facebook Accounts erarbeitet. Nach Auffassung von IDC besteht aber in vielen Unternehmen nicht nur bei der Nutzung von Facebook, sondern auch bei weiteren Tools besteht deutlicher Handlungsbedarf. Gehen Sie mit diesen Themen proaktiv um.

IDC Empfehlungen

Sie als Verantwortliche für IT-Sicherheit haben es in der Hand, Ihr Unternehmen bestmöglich abzusichern. Aus Sicht von IDC sollten als Basis für eine hohe Sicherheit folgende Aspekte berücksichtigt werden:

- Halten Sie die Signaturen und Patches immer hochaktuell und setzen Sie die empfohlenen Engines und Applikationen ein.
- Nutzen Sie Standards und Best Practices zur Ausgestaltung Ihrer Sicherheitsarchitektur und Sicherheitskonzepte und überprüfen Sie Ihre Konzepte regelmäßig.
- Sensibilisieren Sie sowohl die Führungskräfte als auch die Mitarbeiter und Beschäftigten Ihres Unternehmens für Sicherheitsbelange.

Auf Basis der Befragungsergebnisse empfiehlt IDC Anwenderunternehmen folgendes:

Verfolgen Sie einen ganzheitlichen Sicherheitsansatz

Jedes Unternehmen hat seine ganz spezifischen Sicherheitsanforderungen. Diese Anforderungen müssen so umgesetzt werden, dass viele Arten möglicher Angriffe auf die IT effektiv abgewehrt werden. Dabei gilt es insbesondere, die individuellen Gefährdungspotenziale der Unternehmen zu berücksichtigen. Auch die Motivationen der Angreifer können sehr vielfältig sein und mit unterschiedlichen Methoden und Technologien vorgetragen werden.

Verfolgen Sie ein ganzheitliches Konzept. Erfassen Sie die Bedrohungslage Ihres Unternehmens vollständig und umfassend und richten Sie die Sicherheitsmaßnahmen und -komponenten unter einem gesamtheitlichen Ansatz aus. Zudem sollten Sie einen effektiven Prozess zur Gewährleistung der IT-Sicherheit etablieren. Dabei muss klar sein, dass IT-Sicherheit kein Projekt mit einem klar umrissenen Anfang und Ende ist.

Verbessern Sie die Mitarbeitersensibilisierung

Unternehmen betrachten die Anwender als ein schwaches Glied innerhalb der Security-Kette. Und tatsächlich entstehen viele Sicherheitsrisiken durch die Anwender innerhalb eines Unternehmens.

Oftmals wird IT Security nur als lästige Pflicht wahrgenommen, die ein effektives Arbeiten erschwert. Daraus erwachsen Nachlässigkeiten, die durchaus eine Gefahr für das Unternehmen darstellen können. Sicherheitsmaßnahmen greifen aber nur dann, wenn die Sicherheitskonzepte auch von jedem einzelnen Mitarbeiter gelebt werden.

Stärken 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.

Sicherheitsrichtlinien und eine Sensibilisierung der Mitarbeiter sind unumgänglich, um einen wirksamen Schutz des Unternehmens zu gewährleisten.

Treiben Sie Sicherheit im Cloud Computing voran

Cloud Computing ist einer der wichtigsten Trends in der IT. 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.

Cloud Services stellen hohe Anforderungen an IT-Sicherheitskonzepte und deren Umsetzung. Achten Sie insbesondere auf Netzwerksicherheit, Identity- und Access Management sowie Endpoint Security.

Schützen und integrieren Sie mobile Lösungen

Der Anteil der mobilen Nutzer und mobile Geschäftsszenarien wachsen rasant. Die Absicherung mobiler Endgeräte muss Bestandteil Ihrer gesamten Sicherheitslösung sein und in die Sicherheitskonzepte integriert werden.

Achten Sie auf die zunehmende Komplexität der Sicherheitslösungen im Bereich Mobility und legen Sie Wert auf Investitionssicherheit.

Die Nutzer mobiler Endgeräte sollen die Sicherheitskonzepte für mobile Lösungen nachvollziehen können. Die Akzeptanz des Nutzers steigt bzw. ist nur dann gegeben, wenn er versteht, warum bestimmte Sicherheitsmaßnahmen ergriffen werden.

Social Media und Web 2.0 sicher nutzen

Viele Firmen nutzen bereits Social Media und Web 2.0 und beschäftigen sich nun zunehmend mit sicherheitsrelevanten Fragestellungen. Sensibilisieren Sie Ihre Mitarbeiter für die Risiken und Gefahrenpotenzial von Social Media und Web 2.0. Hierzu zählen u.a.

- Diebstahl von Identitäten, Vorspiegelung falscher Identitäten
- Verbreitung nicht zulässiger/kompromittierender Informationen durch die Anwender
- Platzierung von Schadcode durch Angreifer.

Führen Sie Awareness-Kampagnen durch und implementieren Sie Sicherheitskonzepte, die speziell auf Social Media und Web 2.0 abzielen. Auch bei Social Media müssen Sie Identity Management und Access Management beachten. Prüfen Sie zudem, in welcher Form IT Security von Social Media und Web 2.0 in die unternehmensweite IT-Sicherheitskonzeption integriert werden können.

Empfehlungen von Anwendern für Anwender

Im Rahmen der Befragung wurden die Unternehmen von IDC gefragt, welches die drei gefährlichsten Angriffsszenarien sind. Die Antworten waren erwartungsgemäß unterschiedlich und teilweise auch sehr unternehmensspezifisch.

Nachfolgend sind einige Aspekte dargestellt, auf die die befragten Anwender im speziellen hinweisen und deren Beachtung auch für andere Unternehmen nützlich sind:

- "Hackerangriffe von außen, Datendiebstahl von innen, Manipulation von innen"
- "Hacking, Trojaner, Würme und Viren, Datenverlust"
- "Industriespionage, Datenverlust durch Mitarbeiter, Angriffe auf Cloud Services"
- "Ausfall des Gesamtsystems, Verlust von Kundendaten, Angriffe auf die Produktentwicklung"
- "DoS, gezielter Virenangriff, Netzwerksabotage"
- "Externe Angriffe auf Smartphones, externe Angriffe auf Tablets, neue Bedrohungsqualität durch Malware"
- "Rufschädigung durch peinliche Social Media Einträge von Mitarbeitern"
- "Serverattacken, Identitätsdiebstahl, Viren".

METHODIK

Bei dem vorliegenden Dokument handelt es sich um einen Auszug aus der Multi-Client-Studie "IT Security in Deutschland 2011 – Neue Herausforderungen durch Cloud Computing, Mobilität und Social Media", die u.a. von Siemens Enterprise Communications GmbH & Co. KG gesponsert wurde.

Im Juni 2011 führte IDC eine primäre Marktbefragung bei 202 Unternehmen mit mehr als 100 Mitarbeitern zu diesem Thema durch. Es wurden hauptsächlich Fach- und Führungskräfte in die Stichprobe aufgenommen, in deren Verantwortungsbereich das Thema IT-Sicherheit fällt.

Die Darstellung des Unternehmensprofils sowie der Produktinformationen basiert auf Informationen, die von Siemens Enterprise Communications zur Verfügung gestellt wurden. Für diese Angaben übernimmt IDC keine Gewähr.

Fallstudie: Sportcast GmbH

Informationen zum Kunden

Sportcast GmbH ist einer der weltweit größten Produzenten von Live-Sport in HD und als Tochterunternehmen der DFL Deutsche Fußball Liga GmbH Hostbroadcaster der Bundesliga und zweiten Bundesliga. Daneben produziert Sportcast alle Spiele des DFB-Pokals und steht im Bereich der multimedialen Produktion weiteren Verbänden und Ligen als kompetenter Ansprechpartner zur Seite.

Sportcast ist TV-Mediendienstleister und Kompetenzzentrum für die Produktion und Durchführung von Sport-TV-Veranstaltungen. Sie analysieren Produktionsumfänge, definieren das ideale Zusammenspiel aller Beteiligten und unterstützen die reibungslose Umsetzung. Im Vordergrund steht dabei ein systematisches Qualitätsmanagement, das eine durchgängige Produktionssicherheit sowie ein exzellentes Endprodukt gewährleistet. Höchste Qualität, Sicherheit und gezielte Innovation sind die Eckpfeiler für die internationale Maßstäbe setzenden, hochkarätigen Sport-TV-Produktionen der Sportcast GmbH.

Anforderungen des Kunden

Um den stetig wachsenden Anforderungen an eine durchgängige Produktionssicherheit gerecht zu werden, ist eine hochverfügbare und sichere IT Infrastruktur zwingend erforderlich. Da die eingesetzte eSieNet-Lösung für VPN und Mail-Gateways sowie die räumlichen Gegebenheiten des Rechenzentrums sowohl an Kapazitäts- als auch an Performancegrenzen stießen, wurde Siemens Enterprise Communications beauftragt, ein stimmiges Gesamtkonzept für die Netzwerk- und Security Infrastruktur, die Virtualisierung der Serverlandschaft und die Entwicklung von Prozess-unterstützenden Web-Applikationen für die Zusammenarbeit mit Partnern zu entwickeln und umzusetzen.

Darstellung der Lösung

Das Multilayer- und Multivendor-Sicherheitsdesign von Siemens Enterprise Communications Professional Services integrierte Ironport Appliances zu Web- und Content Security, CheckPoint Appliances zur Absicherung der Netzwerkbereiche bei hohen Datenflüssen, ein Virtualisierungskonzept mit VMWare und zentraler Storage Server mit NetApp, ein SharePoint Portal als zentraler Informationsdrehscheibe sowie Enterasys Netzwerk-Komponenten zu einem ganzheitlichen Gesamtkonzept.

Die zielgerichteten, auf die Bedürfnisse der Sportcast zugeschnittenen State of the Art Security Lösungen, das innovative Virtualisierungskonzept, die hochperformante Netzwerk Infrastruktur sowie ein zentrales Back-Up-Konzept gewährten Produktionssicherheit und Hochverfügbarkeit für die Produktion und Durchführung von Sport TV-Veranstaltungen und stellten sicher, dass Kunden und Partner der Sportcast GmbH ein hochwertiges Endprodukt erhalten.

Ein zentrales – durch ausgelagerte Managed Services betreutes – SharePoint Web-Portal optimierte die Prozesse und verbesserte die Informationsflüsse zu Partnern und Kunden.

Darüber hinaus ergaben sich deutliche Kosteneinsparungen: Durch Virtualisierung konnte der ansonsten notwendig gewordenen Neubau eines Rechenzentrums vermieden und der Energieverbrauch nachhaltig reduziert werden

Projekt Highlights

- Hochverfügbarkeit und Sicherheit durch innovative Netzwerk-Infrastruktur, verbunden mit State of the Art Security Lösungen.
- Kostenreduzierung durch Virtualisierung der Server-Farm.
- Prozessoptimierung durch ein zentrales SharePoint-Portal als Informations-drehscheibe aller angebotenen Web-Portale.
- Gewährleistung der durchgängigen Produktionssicherheit und Sicherstellung eines ausgezeichneten Endprodukts für die Kunden und Partner der SportCast GmbH

Zitate des Kunden zum Projekt

- „Siemens Enterprise Communications hat es verstanden, unseren Anspruch - Höchste Qualität, Sicherheit und gezielte Innovation - mit einem umfangreichen und auf unsere Bedürfnisse zugeschnittenen Sicherheitskonzept umzusetzen.“

Dirk Fußwinkel, IT Manager Sportcast GmbH

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, 2011. Die Vervielfältigung dieses Dokuments ist ohne schriftliche Erlaubnis strengstens untersagt.