Forschung

Ein andauerndes Sicherheitsparadoxon

Dritte weltweite Studie zum Kostenvergleich reaktiver und präventiver Sicherheitsstrategien in mittelständischen Unternehmen

Eine Forschungsarbeit von Bloor Research
Autor: Nigel Stanley
Veröffentlichungsdatum: September 2010

Bedrohungen treten in vielen Formen und in unterschiedlichen Ausmaßen auf, stellen aber in allen Fällen eine Gefahr für ein Unternehmen dar.

Nigel Stanley

Vorwort

Internetkriminelle, Hacker, Malware. Nur ein paar der Bedrohungen, denen sich mittelständische Unternehmen weltweit gegenübersehen. Diese Bedrohungen sind nicht nur lästig, weil sie Menschen von der Arbeit abhalten, sondern können sehr reale, konkrete und schädliche Auswirkungen für ein Unternehmen mit sich bringen. Ausmaß, Vielfältigkeit und Anzahl dieser Bedrohungen wachsen Jahr um Jahr: 2009 bewerteten die McAfee® Labs beispielsweise mehr als 27 Millionen Domains und fanden heraus, dass fast 6 % davon ein Risiko darstellten, gegenüber 4 % der 9,9 Millionen Webseiten, die 2008 analysiert worden waren (Quelle: McAfee Security Journal 2010). Durch diesen gewaltigen Anstieg der Risiken stehen mittelständische Unternehmen, die ihre Erträge angesichts des Wettbewerbsdrucks und der nur sehr langsam einsetzenden Erholung von der weltweiten Finanzkrise zu steigern versuchen, zusätzlich unter Druck.

Die IT-Generalisten in mittelständischen Unternehmen stehen vor einem Paradoxon: Einerseits soll ein Unternehmen in die Lage versetzt werden zu wachsen, neue geschäftliche Möglichkeiten zu entwickeln und neue Wege zur Geschäftsabwicklung zu beschreiten, andererseits sollen gleichzeitig die Unternehmensressourcen und Unternehmensdaten trotz begrenzter Ressourcen und eines begrenzten Budgets geschützt sein. Wachsende Bedrohungen, schrumpfende Budgets - das ist ein „Sicherheitsparadoxon", wie es im letztjährigen Bericht genannt wurde.

Aber die Unternehmen haben es nicht nur mit Bedrohungen von außen zu tun. In vielen Fällen geht die Gefahr von bislang vertrauenswürdigen Mitarbeitern aus, die Kundendaten, Finanzdaten oder Produktpläne entwenden. Ein privilegierter Zugang zu internen Daten und ein verärgerter Mitarbeiter ergeben eine verhängnisvolle Kombination und stellen ein ernstes Problem dar, das es zu lösen gilt. In der Vergangenheit wurden häufig Versuche zur Vertuschung solcher Mißbräuche unternommen, jedoch machen es gesetzliche Vorgaben und die Kontrolle der Compliance ebenso wie die Entwicklung des Social Networking erforderlich, derartige Ereignisse allgemein bekannt zu machen. Die Wahrung des guten Rufs ist mittlerweile ein wichtiges Thema.

In diesem Bericht werden, wie schon im Vorjahr, die Sicherheitsausgaben mittelständischer Unternehmen (51 bis 1.000 Mitarbeiter) untersucht. Natürlich unterscheiden sich Struktur und Möglichkeiten eines Unternehmens mit 51 Mitarbeitern erheblich von einem Unternehmen, das 1.000 Mitarbeiter beschäftigt. Beide stehen jedoch vor der gleichen Herausforderung, nämlich dem möglichst kostengünstigen Umgang mit Bedrohungen der IT-Sicherheit.

Diese Bedrohungen sind absolut real. 83 % der Unternehmen geben an, dass sie besorgt oder sehr besorgt sind, Ziel eines schädlichen Angriffs auf die IT-Sicherheit zu werden. 51 % der Unternehmen waren bereits Opfer von Angriffen, 16 % davon benötigten mehr als eine Woche zur Behebung eines Problems. 4 % der Unternehmen brauchten dafür sogar mehrere Monate, was für ein mittelständisches Unternehmen eine erhebliche Beeinträchtigung des Geschäftsbetriebs bedeutet. Datenverlust war die häufigste Folge eines Angriffs.

Aber es gibt nicht nur Negatives zu berichten.

Anbieter von IT-Sicherheitslösungen arbeiten nach wie vor intensiv an der Entwicklung von Lösungen, die das Schadensrisiko für Unternehmen durch Internetkriminelle und Hacker mindern. Durch die Implementierung einer gut durchdachten und verwalteten IT-Sicherheitslösung können Unternehmen das Risiko, Opfer eines Angriffs zu werden, deutlich verringern. Auf diese Weise kann sich ein Unternehmen auf seine wichtigsten Ziele wie die Entwicklung neuer Geschäftsmöglichkeiten in dieser wichtigen Phase der konjunkturellen Erholung konzentrieren.

Vorgehensweise

Die Umfrage wurde von Bloor Research im Auftrag von McAfee durchgeführt. Über 1.100 Fragebögen wurden von Personen ausgefüllt, die die folgenden Kriterien aufweisen:

- Mitarbeiter in einem Unternehmen mit 51 bis 1.000 Beschäftigten weltweit
- zuständig für IT-Einkauf, IT-Management oder gesamtverantwortlich für Governance, Risiko- und Compliance-Management im Unternehmen
- angestellt im privaten Sektor (also nicht in Behörden, im Bildungsbereich oder bei Non-Profit-Organisationen).

Die Umfrage wurde sowohl telefonisch als auch über das Internet in den folgenden Ländern durchgeführt:

Australien	Brasilien	Kanada
China	Frankreich	Deutschland
Indien	Japan	Mexiko
Niederlande	Neuseeland	Spanien
Großbritannien	USA	

Die Daten wurden zur Analyse für die folgenden geografischen Bereiche zusammengefasst:

- Asien-Pazifik-Raum (APAC)
- Lateinamerika (LTAM)
- Europa, Nahost und Afrika (EMEA)

Wichtige Ergebnisse weltweit

54 % der mittelgroßen Unternehmen stellen für sich ein Anwachsen der Sicherheitsrisiken im IT-Bereich von 2009 bis 2010 fest, eine Steigerung um 2 % gegenüber dem Vorjahr.

40 % der mittelgroßen Unternehmen berichten von Verletzungen der Datensicherheit im zurückliegenden Jahr, eine Steigerung um 13 % gegenüber dem Vorjahr.

75 % der mittelgroßen Unternehmen geben an, dass eine schwerwiegende Verletzung der Datensicherheit das Unternehmen in seinem Bestand gefährden könnte. Das bedeutet eine Steigerung gegenüber dem Ergebnis der letztjährigen Umfrage (70 %).

30 % der mittelgroßen Unternehmen hatten es bereits mehrfach mit Sicherheitsvorfällen im Netzwerk zu tun, in 55 % dieser Fälle nahmen Untersuchung und Problembehebung bis zu 5 Stunden in Anspruch.

58 % der Umfrageteilnehmer aus der ganzen Welt arbeiten weniger als 3 Stunden wöchentlich an der IT-Sicherheit und beschäftigen sich mit deren Bewertung und Untersuchung. Im vergangenen Jahr waren es noch 65 %.

5 % der mittelgroßen Unternehmen berichten von Datenverlusten, die Kosten von mehr als 25.000 Dollar verursachten. Von diesen Unternehmen befinden sich 25 % in China, 14 % in Frankreich und 11 % in Indien.

47 % aller gemeldeten Fälle von Diebstahl geistigen Eigentums betreffen mittelständische Unternehmen aus dem Wirtschaftsraum EMEA.

88 % der mittelgroßen Unternehmen geben an, dass sie besorgt oder sehr besorgt sind bezüglich Sicherheitsvorfällen, die versehentlich hervorgerufen wurden.

60 % der mittelgroßen Unternehmen weltweit geben zu, weniger als 75 % der gesetzlichen und zur Einhaltung der Richtlinienkonformität in ihrem Unternehmen gebotenen Maßnahmen zu kennen.

Analyse von Bedrohungen, Vorfällen und Reaktionen

Bedrohungen treten in vielen Formen und in unterschiedlichen Ausmaßen auf, stellen aber in allen Fällen eine Gefahr für Unternehmen dar. Die Befragten wurden gebeten, eine Angabe zur Zahl der Sicherheitsvorfälle zu machen, die in den vergangenen drei Jahren bei ihnen aufgetreten sind und diese nach Vorfällen ohne schädigende Absicht (Beispiel: verlorener Laptop) und Vorfällen mit schädigender Absicht (Beispiel: Versuch eines gezielten Hackerangriffs) zu unterscheiden. Interessanterweise geben 53 % der Befragten an, von 1 bis 5 Vorfällen ohne schädigende Absicht betroffen gewesen zu sein, und 46 % sind Opfer von 1 bis 5 Vorfällen mit schädigender Absicht geworden. Es ist ermutigend zu erfahren, dass 17 % der Befragten weder den einen noch den anderen Fall erlebt haben, was den Schluss zulässt, dass sie über gute Schutzmechanismen verfügen oder einfach Glück hatten. Höchstwahrscheinlich war es eine Kombination aus beidem.

Die häufigste Bedrohung, mit der es die Unternehmen zu tun bekamen, war in 16 % Malware auf PCs und Laptops, direkt gefolgt von Schadcode in E-Mail-Anhängen (15 %). Bei den Befragten, die darüber hinaus 21 Bedrohungen und mehr im Laufe des Jahres angeben, entfallen 41 % auf E-Mail-Bedrohungen – auch hier geht es also um Schadcode in E-Mail-Anhängen. Offensichtlich waren einige Unternehmen nicht in der Lage, nach einem Einbruch in ihr IT-System die erforderlichen Gegenmaßnahmen zu treffen und wurden so Opfer mehrerer Folgeangriffe.

Webseiten-Bedrohungen (wie Phishing-Angriffe, Hacker- und Web-2.0-Angriffe) machen nach Angaben der mittelständischen Unternehmen 12 % aller Bedrohungen aus, und 10 % aller Vorfälle hatten für das betroffene Unternehmen einen Datenverlust zur Folge.

Die Berichterstattung über Datenlecks und Datenschutzverstöße ist mittlerweile in vielen Ländern gesetzlich vorgeschrieben. Die Gefahr, dass ein solcher Vorfall öffentlich bekannt wird sowie das damit verbundene Reputationsrisiko zwingt auch sonst zögerliche Unternehmen dazu, Maßnahmen zum Datenschutz zu ergreifen. Hinzu kommt die Tatsache, dass der Gesetzgeber bei Datenpannen mittlerweile empfindliche Bußgelder verhängen kann, so dass es wenig überraschend ist, wenn Mittelständler zu dem Schluss kommen, dass sie sich Datenverluste einfach nicht mehr leisten können.

40 % der Befragten geben an, dass sie einen Fall von Verletzung der Datensicherheit erfahren haben, 5 % sagen aus, dass es häufig oder sogar sehr häufig zu Datenverlusten gekommen ist. Im Vergleich dazu berichten 29 % der im vergangenen Jahr befragten Unternehmen von Verletzungen der Datensicherheit. Diese Steigerung ist wahrscheinlich auf gezieltere Angriffe zurückzuführen, die dem Diebstahl bestimmter Unternehmensdaten sowie geistigen Eigentums dienen. Eine ganze Branche hat sich rund um den Kauf und Verkauf von Unternehmensdaten entwickelt. Interessanterweise geben nur 6 % der Befragten an, im vergangenen Jahr einen veröffentlichungspflichtigen Datenverlust erlitten zu haben, was möglicherweise auf die entsprechenden gesetzlichen Regelungen zurückzuführen ist, denen sie unterliegen.

Mittelständische Unternehmen aus Europa, dem Nahen Osten und Afrika (EMEA) sowie dem asiatisch-pazifischen Raum (APAC) sind in der Kategorie der Unternehmen mit häufigen Datenverlusten stark vertreten – in einigen Fällen weisen sie fünfmal mehr Vorfälle auf als nordamerikanische Unternehmen vergleichbarer Größe.

Das Ausmaß des entstandenen Datenverlustes ist sehr unterschiedlich, am häufigsten handelt es sich jedoch um personenbezogene Daten (Mitarbeiter- oder Kundendaten), die 26 % der Befragten nennen, gefolgt von geistigem Eigentum (23 %) und Geschäftsplänen (16 %). 47 % aller gemeldeten Fälle von Diebstahl geistigen Eigentums betreffen mittelgroße Unternehmen aus dem Wirtschaftsraum EMEA, verglichen mit lediglich 13 % aus Nordamerika (NA). 41 % der Verlustfälle in Bezug auf personenbezogene Daten tangieren Unternehmen aus dem Wirtschaftsraum EMEA, 15 % der Unternehmen sind in Nordamerika, 21 % im Wirtschaftsraum APAC ansässig. Im vergangenen Jahr entfielen 40 % der gestohlenen Daten auf personenbezogene Daten von Kunden, Mitarbeitern und Geschäftspartnern.

Analyse von Bedrohungen, Vorfällen und Reaktionen

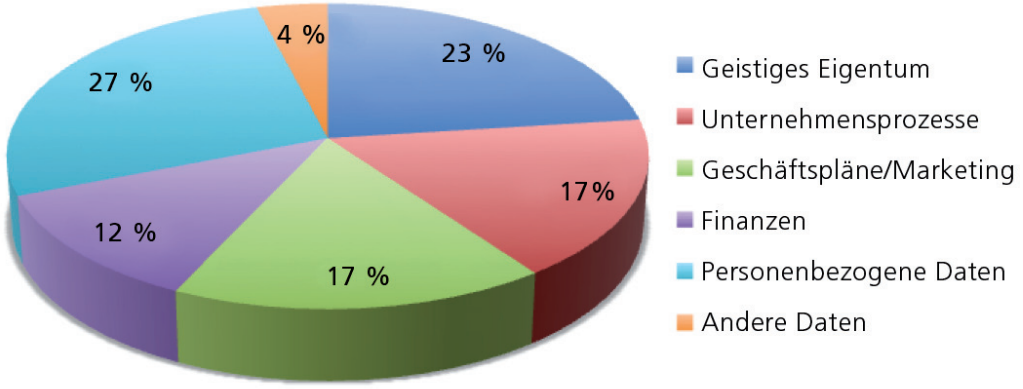

Abbildung 1: Welche Arten von Daten wurden Ihnen entwendet?

Die Kosten, die durch Verletzungen der Datensicherheit entstehen, sind für jedes Unternehmen signifikant, und 5 % der Mittelständler berichten, dass sie einen Datenverlust erlitten haben, der Kosten von mehr als 25.000 Dollar verursacht hat. Von diesen Unternehmen sind 25 % in China, 14 % in Frankreich und 11 % in Indien ansässig. Noch entscheidender allerdings: 75 % der mittelgroßen Unternehmen geben an, dass eine schwerwiegende Verletzung der Datensicherheit das Unternehmen in seinem Bestand gefährden könnte. Im vergangenen Jahr lag dieser Wert bei 70 %, so dass also inzwischen noch mehr Unternehmen über die Auswirkungen eines Datenverlustes nachdenken.

Bei den Unternehmen, die von bis zu 5 Vorfällen berichten, waren 30 % auf Malware, entweder direkt am Endgerät oder über E-Mail verbreitet, zurückzuführen. Da E-Mail ein unverzichtbares Tool im Geschäftsverkehr darstellt, wird dieser Dienst gern von Internetkriminellen für Datendiebstahl genutzt, zumal ein E-Mail-Anhang durch geschicktes Social Engineering so gestaltet werden kann, dass er von vielen Benutzern geöffnet wird.

Eine weitere aktuelle Entwicklung sind die Bedrohungen, die im Zusammenhang mit Cloud Computing entstehen. Die Bereitstellung "in the cloud" von IT-Infrastruktur, Software oder Diensten erhält derzeit viel Aufmerksamkeit, da die Datenverarbeitung an eine Drittpartei ausgelagert wird, was IT-Kosten spart. Auf diese Weise kann sich ein mittelgroßes Unternehmen auf sein Kerngeschäft konzentrieren und auf eine umfangreiche IT-Infrastruktur verzichten. Natürlich sehen Internetkriminelle die entstehenden Datenströme und deren externe Verarbeitung als Möglichkeit, Sicherheitslücken zum Datendiebstahl auszunutzen, und wir rechnen mit einem Anstieg derartiger Vorfälle. Bereits 4 % der weltweit Befragten berichten von bis zu 10 Vorfällen im Zusammenhang mit Cloud Computing im vergangenen Jahr, und 54 % davon sind mittelständische Unternehmen aus dem Wirtschaftsraum EMEA. Outsourcing bedeutet also keineswegs, dass Risiken ebenfalls ausgelagert werden.

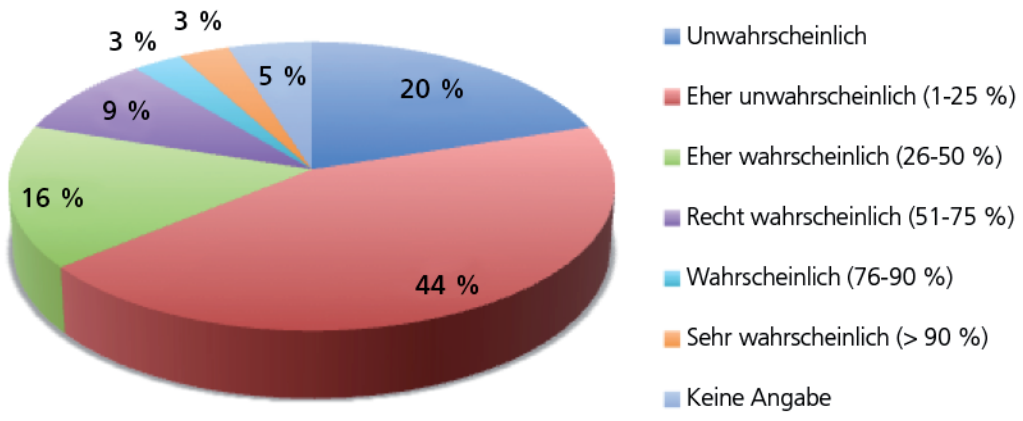

Abbildung 2: Wie hoch schätzen Sie die Wahrscheinlichkeit ein, dass durch eine schwerwiegende Verletzung der Datensicherheit auch Ihr Unternehmen in seinem Bestand gefährdet werden könnte?

Analyse von Bedrohungen, Vorfällen und Reaktionen

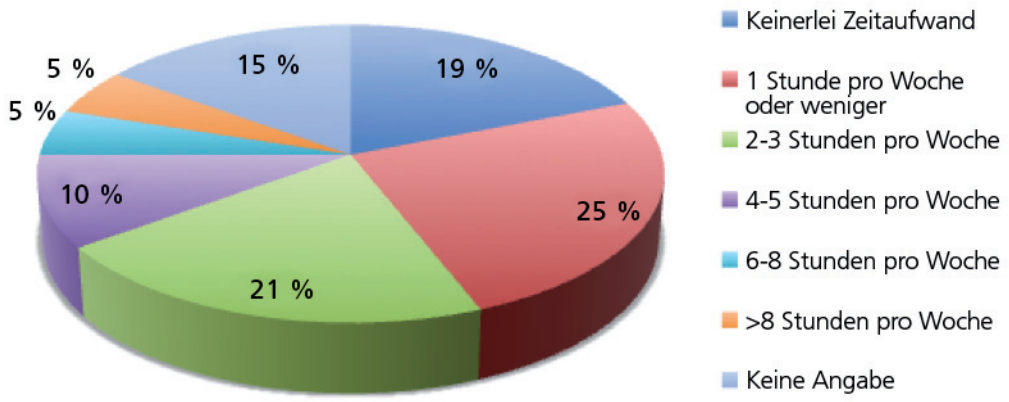

Abbildung 3: Wie lange dauert die Untersuchung und Problembehebung bei einem Vorfall im Netzwerk ungefähr?

Neue Untersuchungsbereiche im diesjährigen Bericht sind die zunehmenden Sicherheitbedrohungen, die von Anwendungscode und Mobiltelefonen ausgehen. Anwendungscode wird häufig von Hackern genutzt, die auf der Suche nach einer Lücke in der Sicherheitsinfrastruktur sind. Es ist sehr schwierig, Programmcode so zu schreiben, dass keine Sicherheitslücken bestehen, und da mittelständische Unternehmen häufig Programmcode und Anwendungen von Dritten einkaufen, besteht ein zunehmender Bedarf sicherzustellen, dass die Software keine Sicherheitslücken hat.

Mobiltelefone und Smartphones verfügen über immer mehr Rechenleistung, so dass ein Smartphone heute bereits mit einem PC vergleichbar ist. Im vergangenen Jahr war ein Anstieg des Hackerinteresses an Mobiltelefonen und Smartphones festzustellen. Diese Angriffe erfolgen meist in Form einer Trojaner-Software – harmlos erscheinende Spiele, die von einer Webseite mit Anwendungen heruntergeladen werden, und die E-Mails, Textmitteilungen und sogar Telefongespräche mit Fehlermeldungen unmerklich abschöpfen. 4 % der Befragten geben für das vergangene Jahr bis zu 10 Verletzungen der Datensicherheit im Bereich Inhalte und Sprachdienste an. In absoluten Zahlen sind das mehr Vorfälle als im Bereich Cloud Computing. In den kommenden Jahren werden Vorfälle dieser Art zwangsläufig noch häufiger werden.

Software-Patches sind immer noch wichtig. Die Anbieter haben ihre Patch-Tests und Bereitstellungszyklen erheblich verbessert, doch immer noch sind von Zeit zu Zeit unangekündigte Patches erforderlich. 46 % der Befragten weltweit mussten im vergangenen Jahr, zusätzlich zu den regelmäßig bereitgestellten Patches, bis zu 3 unangekündigte Patches einspielen.

Netzwerke sind aufgrund ihrer Komplexität und Internetanbindung immer noch anfällig für Angriffe. 39 % der Befragten weltweit hatten es mit bis zu 2 Sicherheitsvorfällen im Netzwerk zu tun, in 55 % dieser Fälle nahmen Untersuchung und Problembehebung bis zu 5 Stunden in Anspruch. In vielen Fällen entsteht diese Verzögerung durch von Hand durchgeführte Arbeiten im Zusammenhang mit der Korrelierung von Netzwerkvorfällen und der Ursachenanalyse.

Die Zeit, die nach einem Vorfall zur Problembehebung benötigt wird, ist entscheidend. Daher wurden die Teilnehmer gefragt, wie viel Zeit ihr Unternehmen nach dem jüngsten IT-Sicherheitsvorfall bzw. Angriff zur Wiederherstellung brauchte. Diese Frage umfasste alle Auswirkungen auf den Geschäftsbetrieb wie die Wiederherstellung von Systemen und – wichtig – die Zeit, in der die Mitarbeiter nicht arbeiten konnten. 47 % der weltweit Befragten, allen voran jene aus Nordamerika und EMEA, geben eine Wiederherstellung innerhalb eines Tages und 35 % innerhalb weniger Tage an. Natürlich hängt dies von der Art des Vorfalls ab sowie von den betroffenen Systemen und den Tools und Mechanismen zur Handhabung eines derartigen Ereignisses. Eine so schnelle Wiederherstellung ist für ein mittelständisches Unternehmen der Nachweis ausgezeichneter Kenntnisse im Bereich der IT-Sicherheit. Demgegenüber geben 16 % der Unternehmen Wiederherstellungszeiten von ein paar Tagen bis zu einigen Monaten an – eine sehr gefährliche Situation für einen Mittelständler. Im vergangenen Jahr sagten 37 % der Unternehmen aus, dass sie 3 oder mehr Tage für die Problembehebung nach einem Angriff auf die IT-Sicherheit benötigten, und 54 % der britischen Unternehmen gelang die Wiederherstellung nach einem Angriff in weniger als einem Tag. In diesem Jahr geben ähnliche britische Unternehmen an, im Schnitt geringfügig mehr Zeit zu benötigen – nur 49 % nennen eine Wiederherstellungszeit von nicht mehr als einem Tag. Im vergangenen Jahr brauchten 40 % der Mittelständler in den Vereinigten Staaten weniger als einen Tag zur Wiederherstellung nach einem Angriff. In diesem Jahr liegt der Wert bei ermutigenden 54 %.

Das neue Gesicht der Bedrohungen

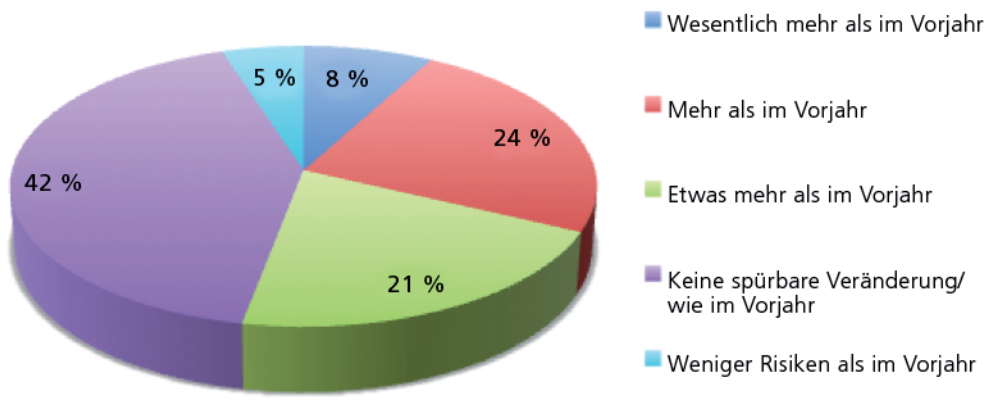

Abbildung 4: In welchem Ausmaß haben sich die IT-Sicherheitsrisiken (Bedrohungen/Vorfälle) in Ihrem Unternehmen von 2009 bis 2010 verändert?

Bedrohungen ändern sich zweifellos von Tag zu Tag. Ständig werden neue Schwachstellen oder Sicherheitslücken bekannt, oder ein Aspekt der IT, der neuerdings Opfer von Angriffen werden kann. Hier die Oberhand zu behalten, ist extrem schwierig und für mittelständische Unternehmen, die in IT-fernen Branchen tätig sind, wahrscheinlich unmöglich. In diesem Zusammenhang muss darauf hingewiesen werden, dass bei der Umfrage 88 % der Mittelständler angeben, besorgt oder sehr besorgt zu sein, was Angriffe auf die IT-Sicherheit ohne schädigende Absicht betrifft und sich 83 % der weltweit Befragten besorgt oder sehr besorgt in Bezug auf schädliche Angriffe auf die IT-Sicherheit äußern. Interessanterweise sind von den sehr besorgten Unternehmen nur 1 % in Japan ansässig, aber 13 % in EMEA und 9 % in Nordamerika.

Den mittelgroßen Unternehmen ist die Gefährdung ihrer Computersysteme sehr wohl bewusst. Dies lässt sich aus der Tatsache ableiten, dass 54 % der weltweit Befragten angeben, dass zwischen 2009 und 2010 die Risiken für ihr Unternehmen im Bereich IT-Sicherheit zugenommen haben. In der Vorjahresstudie lag der Prozentsatz bei 56 %, es handelt sich also um einen bemerkenswert konstanten Wert. Von den Befragten, die sogar sehr viele neue Risiken sehen, sind 39 % in APAC ansässig. Von den Befragten, die im Grunde keine Veränderungen feststellen können, befinden sich 50 % in EMEA; von jenen, die weniger Risiken als im Vorjahr sehen, sind 35 % in Lateinamerika (LTAM) ansässig.

Die Auffassungen über IT-Sicherheitsrisiken ändern sich. 33 % der Befragten fühlen sich gut vor Angriffen auf die IT-Sicherheit geschützt, dagegen fühlen sich aber 7 % nicht sehr gut oder überhaupt nicht geschützt. Von jenen, die sich sehr gut geschützt fühlen, kommen 52 % aus EMEA. 41 % der Befragten geben an, noch niemals Opfer eines Angriffs auf die IT-Sicherheit geworden zu sein, gegenüber 51 %, die diese Frage bejahen (8 % können dazu keine Angabe machen). 13 % der von einem Angriff auf die IT-Sicherheit Betroffenen stammen aus den USA. 7 % der Unternehmen in den USA können nicht sagen, ob sie bereits angegriffen wurden. Im Vorjahr waren dies nur 5 %, im Jahr davor jedoch 15 %, so dass diesen Unternehmen erfreulicherweise insgesamt ein gleichbleibend vorhandenes Sicherheitsbewusstsein attestiert werden kann.

Nach der Größe der Unternehmen gefragt, die für Angriffe am anfälligsten sind, entschieden sich 16 % für die kleineren Unternehmen mit 2 bis 50 Mitarbeitern. Im vergangenen Jahr gaben fast 50 % der Befragten an, dass Unternehmen mit mehr als 500 Mitarbeitern am stärksten gefährdet seien, Opfer eines Angriffs auf die IT-Sicherheit zu werden – dieser Wert ist jetzt auf 21 % gesunken.

Im Gegensatz dazu sind die Ergebnisse zur Implementierung von Sicherheitstechnologien zu sehen. 15 % der Befragten geben sich damit zufrieden, einen Vorfall abzuwarten, um dessen Auswirkungen dann so schnell wie möglich zu beheben, 35 % sind an gesetzliche Vorschriften und/oder Kundenanforderungen gebunden und müssen daher präventive Maßnahmen ergreifen, und 10 % unternehmen nur das Notwendigste und hoffen, dass nichts geschieht. Von den Vertretern der letztgenannten Gruppe sind 26 % aus EMEA und 27 % in APAC ansässig. Nur 5 % der mittelgroßen japanischen Unternehmen folgen derselben Philosophie.

88 % der Befragten geben an, dass die Integrierbarkeit der erworbenen IT-Sicherheitsprodukte in relevante Technologien „sehr wichtig" oder „ziemlich wichtig" ist, damit Berichte, Analysen und die Kenntnis wichtiger Ereignisse systemübergreifend nutzbar gemacht werden können. 27 % wünschen sich, dass ihre Sicherheitsprodukte Verzeichnisdienste und Protokolle nutzen, zweifellos, damit sie einfacher implementiert und genutzt werden können. 23 % geben an, dass sie Speicherungs-Tools nutzen möchten.

Das neue Gesicht der Bedrohungen

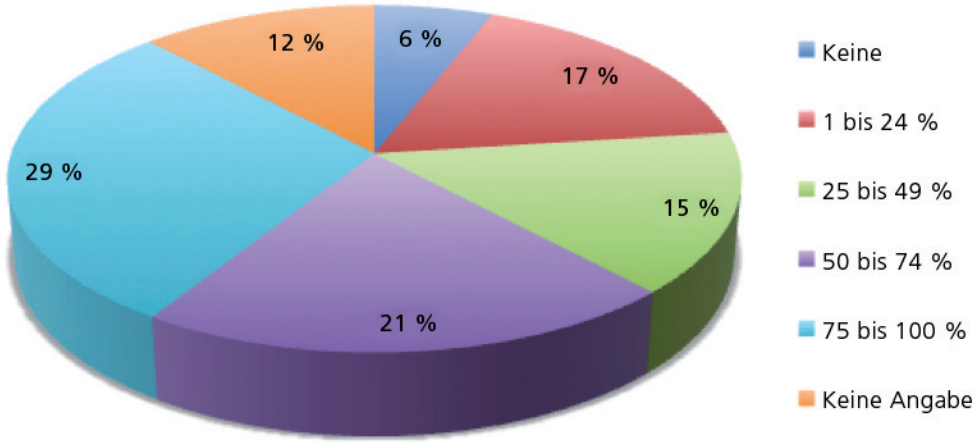

Abbildung 5: Schätzung, wie hoch der Prozentsatz geltender gesetzlicher Regelungen und Compliance-Anforderungen ist, die in den Unternehmen vollständig erfasst und umgesetzt werden

IT-Sicherheit scheint inzwischen ein Bereich zu sein, der auf großes Interesse stößt und in dem intensiv Forschung betrieben wird. 58 % der Umfrageteilnehmer weltweit sagen aus, dass sie weniger als 3 Stunden wöchentlich an der IT-Sicherheit arbeiten und sich mit deren Bewertung und Untersuchung beschäftigen. Im vergangenen Jahr lag dieser Wert bei 65 %, so dass mittelständische Unternehmen insgesamt also offenbar etwas mehr Zeit in die Arbeit an ihren IT-Sicherheitssystemen investieren. 12 % der Befragten geben an, dass sie länger als einen Tag für eine ähnliche Fehlererforschung benötigen. Im vergangenen Jahr verwendeten mehr als 50 % der mittelgroßen französischen Unternehmen weniger als 1 Stunde pro Woche auf präventive Sicherheitsmaßnahmen. In diesem Jahr liegt der Wert bei 28 %. Im vergangenen Jahr gaben 40 % der mittelgroßen chinesischen Unternehmen an, weniger als 1 Stunde pro Woche für präventive Sicherheitsmaßnahmen aufzuwenden gegenüber 26 % in diesem Jahr. In den USA ansässige Unternehmen setzen mehr Zeit für sicherheitsrelevante Aktivitäten ein als Unternehmen in jedem anderen Land. Bei der diesjährigen Umfrage ist dies erneut der Fall.

29 % der Befragten sagten, dass sie über kein Personal verfügen, das sich ausschließlich und ständig mit Sicherheitsfragen beschäftigt, wogegen 51 % angaben, dass sie zwischen 1 und 3 Mitarbeitern in diesem Bereich beschäftigen. 95 % dieser Mitarbeiter wurden als „einigermaßen kompetent" oder „sehr kompetent" klassifiziert, so dass sie in der Lage sind, mit fast allen sicherheitsrelevanten Vorfällen und Situationen umzugehen.

Immer neue gesetzliche Vorschriften bilden den Rahmen für die IT-Sicherheit mittelgroßer Unternehmen und beeinflussen deren Bemühungen und Investitionen in diesem Bereich stark. Es kann sehr schwierig sein, die Vielfalt neuer und geplanter Regeln, Gesetze und Vorgaben zu überblicken. Daher wurden die Umfrageteilnehmer aufgefordert zu schätzen, wie hoch der Prozentsatz geltender gesetzlicher Regelungen und Compliance-Anforderungen ist, die in ihrem Unternehmen vollständig erfasst und umgesetzt werden.

Insgesamt 6 % der weltweit Befragten räumen ein, die für ihr Unternehmen geltenden gesetzlichen Regelungen und Compliance-Anforderungen nicht zu kennen, und nur 29 % geben an, dass ihnen zwischen 75 % und 100 % der geltenden Vorschriften bekannt sind. Von diesen Unternehmen sind 31 % in Nordamerika und 33 % in EMEA ansässig. Hier müssen also auf jeden Fall Maßnahmen ergriffen werden um sicherzustellen, dass mittelständische Unternehmen nicht mit dem Gesetz in Konflikt geraten. Diese gesetzlichen Regelungen sollten außerdem die Sicherheitsausgaben beeinflussen, damit gewährleistet ist, dass die entsprechenden Tools und Technologien bevorzugt behandelt werden.

Damit kommen wir zum allgemeinen Kompetenzniveau des IT-Personals in Unternehmen. Auf einer Skala von „sehr kompetent" bis „überfordert" wird das IT-Personal mehrheitlich (95 %) im Bereich zwischen „sehr kompetent" und „einigermaßen kompetent" verortet. Nur 4 % werden als „überfordert" bezeichnet. Diese Einschätzung ist in allen Regionen und Ländern recht ähnlich, obwohl der Anteil des „sehr kompetenten" IT-Personals in LTAM etwas höher eingeschätzt wurde. Da die Befragten selbst im IT-Bereich arbeiten, ist bei dieser Frage freilich keine ähnlich objektive Antwort wie bei den anderen Fragen dieser Studie zu erwarten!

Das neue Gesicht der Bedrohungen

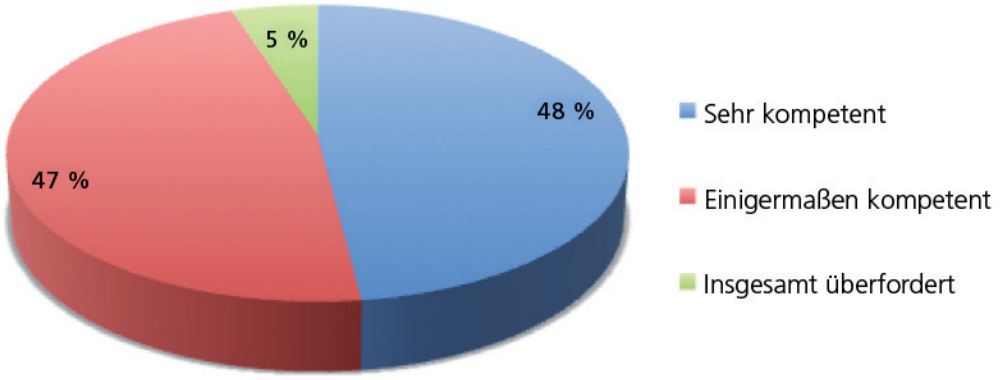

Abbildung 6: Wie würden Sie das allgemeine Kompetenzniveau des IT-Personals in Ihrem Unternehmen beurteilen?

Kosten und Budgets

Budgets spielen heute in jedem Unternehmen eine große Rolle, da angesichts der schwierigen Wirtschaftslage Kostensenkungen an der Tagesordnung sind. Natürlich stehen auch die Ausgaben im IT-Bereich auf dem Prüfstand, direkt gefolgt von den Ausgaben für die IT-Sicherheit. Die Mehrheit der weltweit Befragten (62 %) fasst das Budget für die IT-Sicherheit und das allgemeine IT-Budget zusammen, nur 14 % weisen ein gesondertes Budget für IT-Sicherheit aus. Für viele Unternehmen ist das vielleicht ein sinnvollerer Weg zur Ausweisung der Sicherheitskosten, da diese stark von Compliance-Anforderungen und gesetzlichen Vorgaben beeinflusst werden, denen das Unternehmen insgesamt unterliegt. Die gesonderte Ausweisung eines Budgets für IT-Sicherheit im Haushalt, führt zu einem tiefgreifenderen Verständnis dieses Themas und kann nützlich sein, wenn es um dessen eigenständige Berücksichtigung im Haushalt geht. Die Bandbreite der Budgets, die für IT-Sicherheit veranschlagt werden, ist bemerkenswert. 30 % der Unternehmen können weniger als 10.000 Dollar jährlich aufwenden, einem kleinen Teil (6 %) stehen dagegen mehr als 100.000 Dollar im Jahr zur Verfügung.

Der wirtschaftliche Druck scheint sich nicht allzu negativ auf die Sicherheitsbudgets auszuwirken. Bei 49 % der Befragten hat sich das Budget gegenüber 2009 nicht verändert, 20 % geben eine Steigerung gegenüber dem Vorjahr an, und ebenfalls 20 % müssen mit einem geringeren Budget auskommen. Allerdings sind in keinem Land besonders große Veränderungen festzustellen. Im vergangenen Jahr gaben 75 % der Mittelständler an, ihre Budgets für IT-Sicherheit einzufrieren oder zusammenzustreichen. Außerdem sagte eine Mehrheit der indischen Unternehmen aus, ihre Budgets zu steigern, und nur eine Minderheit plante, sie einzufrieren. In diesem Jahr hat sich der letztgenannte Anteil erhöht, so dass jetzt mehr indische Unternehmen das Budget für IT-Sicherheit eher einfrieren als es zu erhöhen oder zu senken.

Die Entscheidung, das Budget für IT-Sicherheit unverändert zu lassen oder zu erhöhen, spiegelt eine durchdachte Haltung zur IT-Sicherheit seitens der mittelgroßen Unternehmen wider, da die Notwendigkeit erkannt wird, nachhaltig gegen die steigende Zahl von Bedrohungen aus dem Internet vorzugehen, die das Unternehmen gefährden. Interessanterweise sehen 65 % jener Unternehmen, in denen das Budget für IT-Sicherheit gekürzt wurde, darin keine Beeinträchtigung ihrer Sicherheit. 8 % sind bemerkenswerterweise der Auffassung, dass das Sicherheitsniveau durch die Budgetkürzung sogar erhöht wird.

Welche Auswirkungen haben Budgetkürzungen also auf die IT-Sicherheit? 14 % der Befragten äußern, dass sie die Kürzungen zum Umstieg auf kostengünstigere Produkte zwingen (gegenüber 30 % im Vorjahr), 11 % wollen die Arbeitsstunden des IT-Sicherheitspersonals reduzieren (gegenüber ebenfalls 30 % im Vorjahr). Von den Befragten, die eine Reduzierung des IT-Personals bzw. deren Arbeitsstunden planen, sind 22 % in den USA ansässig. Nur 5 % der Befragten geben an, dass die Budgetkürzungen zum Outsourcing ihrer IT-Dienste führen werden. Dabei handelt es sich vor allem um Unternehmen aus Mexiko und Deutschland. 28 % sagen, dass sie den Kauf neuer Sicherheitsprodukte einschränken oder ganz aussetzen wollen (gegenüber 40 % im Vorjahr). Es scheint, dass Budgeteinsparungen die gesamte Palette möglicher Sicherheitsausgaben betreffen.

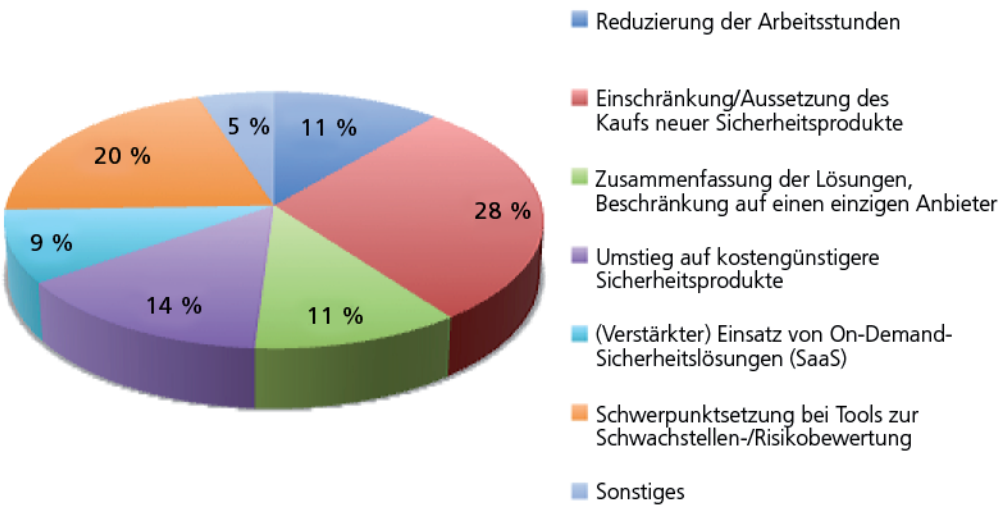

Abbildung 7: Welche Maßnahmen planen Sie 2010 als Reaktion auf die Budgetkürzungen?

Kosten und Budgets

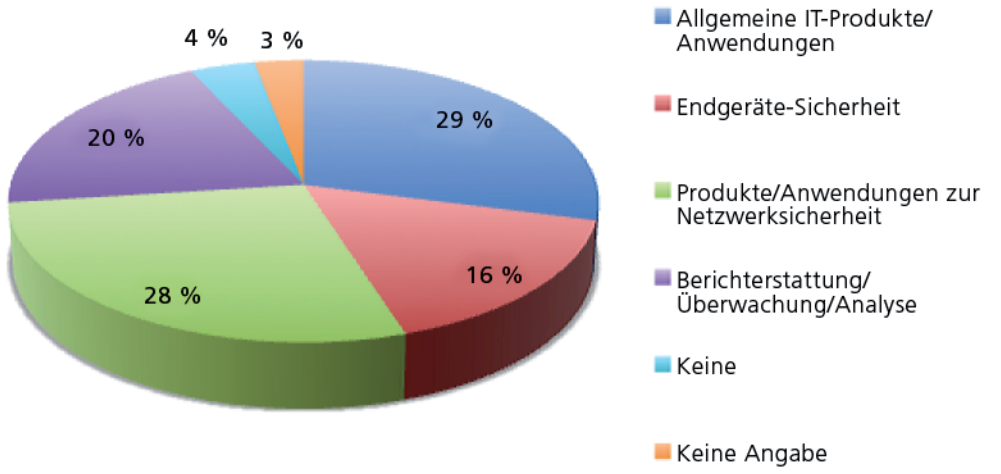

Abbildung 8: In welchen Bereichen ist für Sie Konsolidierung wichtig?

Auf die Frage, welche Produkte sie als Gesamtlösung von einem einzigen Anbieter beziehen würden, nannten 29 % der Befragten „allgemeine IT-Produkte" und 16 % „sicherheitsrelevante Endpoint-Lösungen".

Das Outsourcing von Diensten stellt immer noch ein wichtiges Element der Sicherheitsstrategie dar. Um so interessanter ist die Feststellung, dass diese Möglichkeit immer noch von 27 % der Befragten abgelehnt wird. In allen Regionen wird Outsourcing besonders häufig bei der Schulung des IT-Personals angewandt, und Mittelständler in LTAM nutzen Outsourcing für die Bereiche Fehlerbehebung und Feinabstimmung häufiger als Unternehmen in allen anderen Regionen. Am weitesten verbreitet ist die Verwaltung vor Ort in Nordamerika, insbesondere in den USA.

Trotz der schwierigen Wirtschaftslage werden die Ausgaben für Produkte oder Personal in einigen Bereichen erhöht. 15 % der Befragten geben steigende Ausgaben für den Netzwerkschutz an, 12 % nennen in diesem Zusammenhang den Schutz von E-Mails z. B. durch Spam-Filter. Zu den Bereichen, in denen die Ausgaben gekürzt werden (13 %), zählen der Geräteschutz und Tools zur Verringerung der Gefahr, dass Daten, die sich auf gestohlenen oder verlorenen PCs, Laptops oder Geräten befinden, gestohlen werden.

Alle Sicherheitsbedrohungen oder -ereignisse, denen ein Unternehmen ausgesetzt ist, verursachen bestimmte Kosten.

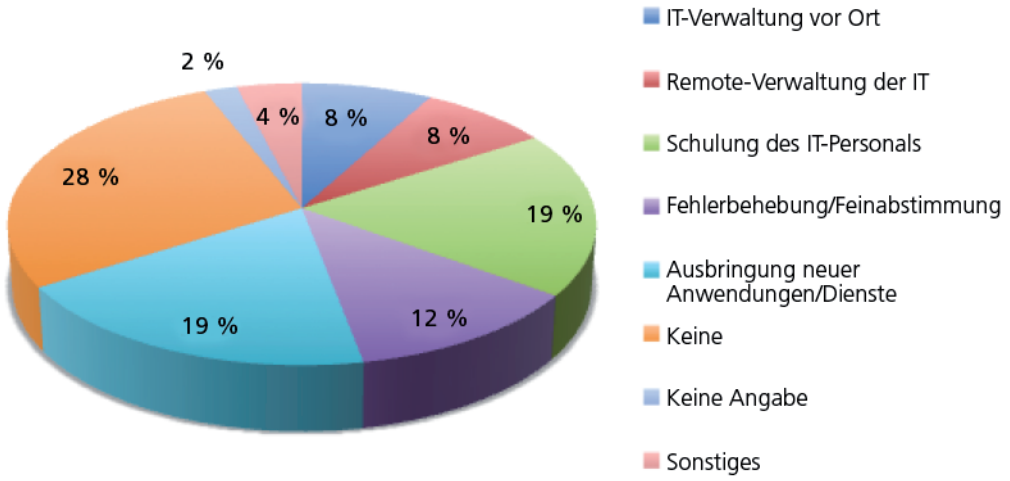

Abbildung 9: Wo nutzen Sie Outsourcing?

Kosten und Budgets

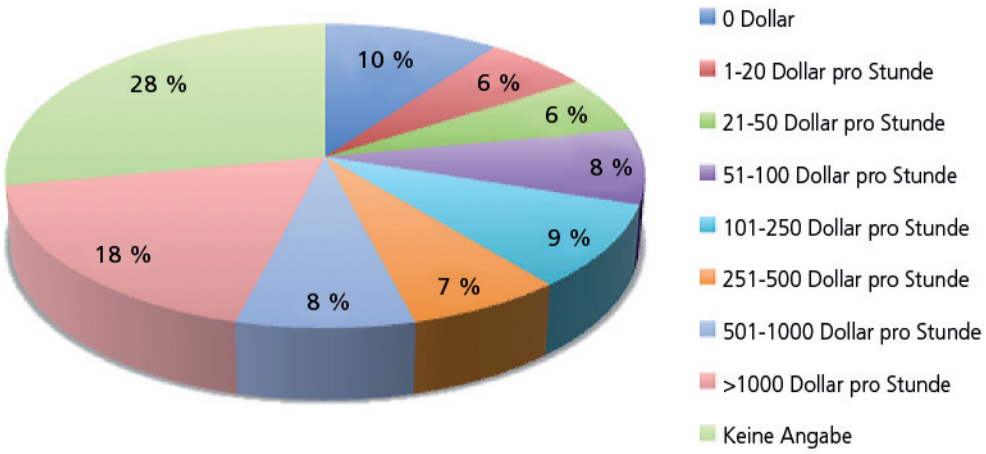

Abbildung 10: Bitte schätzen Sie die Kosten eines Netzwerkausfalls pro Stunde (in US-Dollar)

Die Umfrageteilnehmer wurden gebeten, die Wiederherstellungskosten in US-Dollar nach einem Sicherheitsvorfall oder einem Fall von Malware-Infektion bei einem PC zu schätzen. 10 % der Befragten schätzen die Kosten auf 1 bis 20 Dollar, während der Anteil der Befragten, die Kosten von mehr als 1.000 Dollar angeben, auf 3 % gestiegen ist. Offensichtlich wurde der Wert der Daten auf dem PC hier entweder sehr hoch angesetzt, oder das Unternehmen kann die Entscheidung treffen, angesichts hoher Wiederherstellungskosten auf eine Datenrettung zu verzichten und stattdessen eine Neuanschaffung vorzunehmen.

Netzwerkvorfälle können, gemessen an den Kosten pro Stunde, insbesondere mittelständischen Unternehmen mit begrenzten Ressourcen teuer zu stehen kommen. Bei den befragten Unternehmen verteilen sich die Kosten einigermaßen gleichmäßig auf den Bereich von wenigen Dollar bis 1.000 Dollar pro Stunde, doch 18 % der Unternehmen geben an, dass ihnen für einen Netzwerkvorfall Kosten von mehr als 1.000 Dollar pro Stunde entstanden sind.

Die Umfrageteilnehmer wurden gebeten, die Behebungs- und Wiederherstellungskosten nach einem typischen Vorfall im vergangenen Jahr zu schätzen. Es handelt sich um die Kosten pro Vorfall, wobei Faktoren wie die jeweils genutzten Produkte und Dienste, die Kosten durch den Ausfall des Netzwerks, der zeitliche Aufwand des IT-Personals zur Behebung des Problems usw. eine Rolle spielen. Bei den Vorfällen, die Kosten von mehr als 1.000 Dollar verursachten, sind 19 % auf den Verlust eines Geräts und sensibler Daten zurückzuführen. Die geringsten Kosten für Problembehebung und Wiederherstellung entstanden bei Vorfällen im Bereich E-Mail und in Bezug auf Malware in E-Mail-Anhängen.

Zusammenfassung: Aufbau einer präventiven Verteidigung

Um wieder auf die Füße zu kommen, wettbewerbsfähig zu bleiben und erfolgreich auf dem Markt zu bestehen, bauen mittelgroße Unternehmen bestimmte Bereiche ihrer Geschäftstätigkeit aus: Sie erhöhen die Mobilität ihrer Mitarbeiter, nutzen Möglichkeiten, die Cloud-basiertes Arbeiten bietet oder erschließen mit Hilfe von Web 2.0-Anwendungen neue Märkte. Bei jedem dieser Schritte muss die IT sicherstellen, dass die erforderlichen Prozesse und Richtlinien von einer entsprechenden Sicherheitsinfrastruktur unterstützt werden und Mitarbeiter, Partner sowie Kunden entsprechend geschult und einbezogen werden.

Wie wir in der diesjährigen „Paradox"-Studie gesehen haben, ist es schwierig, hier ein Gleichgewicht zu finden. Im Bereich der IT-Sicherheit muss auf eine sorgfältige Ausgabenplanung geachtet werden, und pauschale Budgetkürzungen sind angesichts der vielfältigen Bedrohungen, denen sich Unternehmen heute ausgesetzt sehen, keine geeignete Maßnahme mehr.

Welche Maßnahmen sollten mittelständische Unternehmen heutzutage also ergreifen?

1. Sie sollten auf jeden Fall eine Bedrohungsanalyse in Echtzeit durchführen können, um mit den wachsenden Gefahren Schritt zu halten.

2. Sie sollten mit Anbietern zusammenarbeiten, die zur Effizienzsteigerung des Sicherheitsmanagements beitragen können, so dass die für manuelle Prozesse benötigte Zeit reduziert wird.

3. Sie sollten interne Richtlinien und Herangehensweisen entwickeln, um sicherzustellen, dass jeder Bedrohungsvektor Berücksichtigung findet.

4. Sie sollten sich um mehrstufige Sicherheitslösungen bemühen, bei denen beispielsweise Virenschutz und Datenverschlüsselung kombiniert werden, so dass nicht jedes Sicherheitsproblem mit Hilfe eines Einzelprodukts gelöst werden muss.

Durch diese durchdachten, zielgerichteten Aktivitäten werden mittelständische Unternehmen in die Lage versetzt, das Sicherheitsparadoxon ein für allemal zu überwinden.

Terminologie und Definitionen

Bei der Zusammenstellung der Daten wurden einige Begriffe und Formulierungen benutzt, die wie folgt definiert sind:

- Ein „Sicherheitsvorfall" liegt dann vor, wenn es zu einer Ausfallzeit, einer Verletzung der Datensicherheit oder einem Datenverlust gekommen ist, der unbeabsichtigt erfolgte. Dazu zählen z. B. der Verlust eines Laptops bzw. USB-Sticks oder eine infizierte Datei, die versehentlich als Anhang einer E-Mail versandt wurde.
- Als „Angriff auf die IT-Sicherheit" gilt der bewusste Versuch, ein System oder die Netzwerksicherheit zu kompromittieren. Dies liegt beispielsweise vor, wenn jemand von außen Daten zerstört, Datendiebstahl begeht, Geräte entwendet oder ein System oder Netzwerk herunterfährt.
- Ein „Datenverlust" liegt vor, wenn einem Unternehmen vertrauliche Daten durch Unachtsamkeit verloren gehen oder diese gestohlen werden.
- „Geräteverlust" bedeutet, dass ein Gerät, das vertrauliche Daten enthält, verloren geht oder gestohlen wird.
- „Endgeräteschutz" umfasst den Schutz von PCs und Laptops vor Malware aller Art.
- „E-Mail-Bedrohungen" sind Schadprogramme oder Schadcode in E-Mail-Anhängen.
- Unter die „Webseiten-Bedrohungen" fallen Phishing- und Hacker-Angriffe gegen Webseiten eines Unternehmens.
- Zu den „Bedrohungen der Netzwerksicherheit" zählen das Hacken von Netzwerken sowie das unbefugte Eindringen in Netzwerke.
- „Bedrohungen durch Anwendungscode" entstehen durch (unabsichtlich verbliebene oder auch absichtlich implementierte) Sicherheitslücken in Programmcode, der intern entwickelt wurde oder von Dritten stammt.
- „Datenbanksicherheit und -überwachung" umfasst die Erkennung und den Schutz angesichts gezielter Angriffe auf Datenbanksysteme, beispielsweise durch Einschleusung von SQL-Code.
- „Mobile Sicherheit" beinhaltet den Schutz vor Verletzungen der Datensicherheit im Bereich Sprachdienste und Inhalte bei Mobiltelefonen.
- Von „Internetbasierten Diensten" ist im Zusammenhang mit der Verletzung der Datensicherheit bei internetbasierten Anwendungen die Rede.
- Zum „geistigen Eigentum" werden Entwürfe, Patente, Formeln, Software und ähnliche Materialien gezählt, die für das Unternehmen einen Wert darstellen.

Weitere Informationen

Weitere Informationen zu diesem Thema erhalten Sie unter
http://www.BloorResearch.com/update/2055

Kurzvorstellung von Bloor Research

Bloor Research ist eines der europaweit führenden IT-Forschungs-, Analyse- und Beratungsunternehmen. Wir erklären, wie sich IT-Systeme in Unternehmen durch effektive Steuerung, Verwaltung und Nutzung von Informationsressourcen flexibler gestalten lassen. Wir haben uns mit unabhängigen, intelligenten, gut ausformulierten Kommunikationsinhalten und Veröffentlichungen zu allen Aspekten der ICT-Branche einen Ruf als Unternehmen aufgebaut, das „die richtige Geschichte erzählt". Dieses „die richtige Geschichte erzählen" beinhaltet unserer Ansicht nach:

- Die Beschreibung der Technologie im Zusammenhang mit ihrem Wert für das Unternehmen und den anderen Systemen und Prozessen, mit denen sie interagiert.
- Verständnis, wie neue und innovative Technologien sich in bestehende ICT-Investitionen eingliedern lassen.
- Betrachtung des gesamten Markts und Erörterung aller verfügbaren Lösungen sowie von Möglichkeiten, diese effektiver zu bewerten.
- Herausfilterung von „Hintergrundrauschen" und Erleichterung der Suche nach zusätzlichen Informationen oder Neuigkeiten, die bei Anschaffung und Implementierung helfen.
- Sicherstellung, dass alle Inhalte von uns über den jeweils am besten geeigneten Kanal vermittelt werden.

Seit der Gründung unseres Unternehmens im Jahr 1989 vermitteln wir seit über zwei Jahrzehnten über Online-Abonnements, maßgeschneiderte Forschungsdienste, Veranstaltungen und Beratungsprojekte Forschungs- und Analyseergebnisse an Unternehmen, die IT-Produkte einsetzen und anbieten. Wir fühlen uns der Aufgabe verpflichtet, unser Know-How in geschäftlichen Nutzen für Sie umzuwandeln.

Über den Autor

Nigel Stanley
Practice Leader – Sicherheit

Nigel Stanley ist Spezialist für Geschäftstechnik und IT-Sicherheit und leitet mittlerweile den Bereich IT-Sicherheit bei Bloor.

IT-Sicherheit umfasst das gesamte Aufgabengebiet im Bereich Schutz und Verteidigung der Systeme und Daten von Unternehmen und Organisationen gegen unerwünschte Angriffe oder unbefugte Netzwerkzugriffe. Dieses umfangreiche Gebiet umfasst Schutzvorkehrungen von den äußeren Zonen des Sicherheitsbereichs (z. B. Handheld-Geräte) über den Netzwerkperimeter bis hin zu internen Bedrohungen und lokalen Abwehrmaßnahmen. Hierbei werden die ständig zunehmenden Bedrohungen untersucht, von denen viele neuartig und ausgefeilt sind. Weitere Aspekte sind der Einsatz von Firewalls, Data Loss Prevention, Datenverschlüsselung, Malware-Schutz, Datenbank-Schutz, Identitätsmanagement, Intrusion Detection/Prevention, Content-Management/-Filterung sowie Sicherheitsrichtlinien und -standards.

Nigel war einige Jahre lang als technischer Leiter bei einem führenden Microsoft-Partnerunternehmen in Großbritannien tätig und führte im Rahmen dieser Tätigkeit ein Team aus Beratern und Technikern bei der Bereitstellung von IT-Lösungen für Unternehmen. Hierzu zählten Data Warehouses, Client-/Server-Anwendungen und intelligente internetbasierte Lösungen. Da mit vielen dieser Lösungen vertrauliche Daten verarbeitet wurden, waren oft zusätzliche Sicherheitsvorkehrungen erforderlich. Von 1995 bis 2003 arbeitete Nigel aufgrund seiner umfassenden Fachkenntnisse über Microsoft-Technologien und Software-Entwicklungstools als Regionsleiter für Microsoft und übernahm in diesem Rahmen beratende Tätigkeiten für die Microsoft Corporation in Redmond.

Nigel hatte bereits zuvor als Systems Engineer und Produktmanager mit dem Spezialgebiet Datenbanken und Entwicklertechnologien für Microsoft gearbeitet. Er war bereits in ganz Europa als führender Experte auf dem Gebiet der Datenbankentwicklung und -implementierung tätig.

Er hat drei Bücher zu Datenbank- und Entwicklungstechnologien wie Microsoft .NET geschrieben. Zurzeit arbeitet er im Auftrag von Unternehmen an einer Reihe von IT-Projekten und ist als Berater für Incoming Thought Limited, einem Partnerunternehmen von Bloor Research, tätig, das sich auf Sicherheitsberatung und -schulungen spezialisiert hat.

Nigel ist Mitglied der Institution of Engineering and Technology, der British Computer Society und des Institute of Directors.

Urheberrechtshinweis & Haftungsausschluss

1. OG,
145–157 St John Street
LONDON,
EC1V 4PY, Großbritannien

Tel.: +44 (0)207 043 9750
Fax: +44 (0)207 043 9748
Internet: www.BloorResearch.com
E-Mail: info@BloorResearch.com