techconsult
The IT Market Analysts

Industrie 4.0 –
Vernetzung braucht IT-Sicherheit

Juni 2013

Titelblatt-Foto von Microsoft Office.com. Verfügbar unter: http://office.microsoft.com/de-de/images/results.aspx?qu=industrie&ex=1#ai:MP900185095|

Inhaltsverzeichnis

Abbildungsverzeichnis

Management Summary

Im Kontext von Industrie 4.0 sind Probleme wie ungesichert aus dem Internet erreichbare Steuerungsanlagen, die in letzter Zeit vermehrt publik wurden, Anzeichen für den Nachholbedarf, der bei der Absicherung von IT-Infrastruktur noch besteht. Bislang sind es nur ein gutes Viertel der Unternehmen, die eine eigenständige IT-Security-Strategie haben und diese auch überprüfen und aktualisieren. Gut die Hälfte behandelt IT-Security nur im Rahmen der allgemeinen IT-Strategie, ein Fünftel der Unternehmen arbeitet überhaupt erst noch an einer IT-Security-Strategie.

Die Absicherung der IT-Infrastruktur verlangt nach einer IT-Strategie, die schon bei der Anschaffung von Hard- und Software ansetzt. Dadurch wird „Security by Design“ angestrebt und der Bedarf an additiven Sicherheitsmaßnahmen, die die Infrastruktur erst im Nachhinein absichert, verringert.

Die IT-Sicherheitsstrategie eines Unternehmens sollte neben als passiv einzustufenden Maßnahmen (z. B. Warten auf Sicherheitsaktualisierungen eines Herstellers) und aktiv-reaktiven Maßnahmen, wie Scans nach Schadsoftware auf potenziell befallenen Systemen, auch proaktiv-präventive Maßnahmen zur Absicherung der IT-Infrastruktur umfassen. Dazu gehört z. B., schon bei der Anschaffung auf zertifizierte Hardware zu achten, die anerkannten Sicherheitsstandards entspricht.

1 Einleitung

Der Trend „Industrie 4.0“ ist zurzeit allgegenwärtig. In Deutschland wurde der Begriff 2013 zum Leitmotto der Hannover-Messe, ist als „Zukunftsprojekt Industrie 4.0“ ein wichtiges Forschungsthema des Bundesministeriums für Bildung und Forschung (BMBF) und wurde auch auf dem just vergangenen 13. Deutschen IT-Sicherheitskongress des Bundesamts für Sicherheit in der Informationstechnik (BSI) diskutiert. Die Kernpunkte, die hinter Industrie 4.0 stecken sind Vernetzung, Automatisierung und Echtzeit-Steuerung/-Analyse in der Fertigungsindustrie. Dabei ist das Thema nicht vollständig neu, sondern kann im Kontext des „Internets der Dinge“ gesehen werden, das als Zusammenwachsen von realer und virtueller Welt entsteht.

Konkret bedeutet Industrie 4.0, dass Maschinen, Produktionsanlagen, ERP-Systeme, Produkte usw. informationstechnologisch vernetzt werden. Als neue Möglichkeiten entstehen mit Industrie 4.0 hochflexible Produktionsprozesse, die in Echtzeit überprüft und gesteuert werden können. Damit können auch die entstehenden Produkte durch den leicht und schnell anzupassenden Produktionsprozess individualisiert werden. Prozesse und Unternehmensbereiche können darüber hinaus noch stärker integriert und Kunden und Lieferanten von Auftrag bis Lieferung eingebunden werden.

Tel.: +49-(0)561-8109-0

Diese hochgradige Vernetzung, die neue Möglichkeiten eröffnet, stellt auf der anderen Seite auch eine potentielle Gefahr dar. Durch die Anbindung an das Internet entsteht die Möglichkeit, weltweit auf diese Geräte zuzugreifen. Eigentlich soll jedoch nicht jeder, sondern nur ein bestimmter Kreis von Personen (z. B. Service-Techniker o. ä.) auf eine Konfigurationsschnittstellt zugreifen können. Es sind also zwingend Sicherheitstechniken notwendig, um die Vorteile der Anbindung an das Internet – zeit- und ortsungebundener Zugriff – mit der Einschränkung des Zugriffs zu kombinieren.

IT-Security wird in diesem Kontext zu einem elementaren Thema für diejenigen Unternehmen, die in Zukunft auf diese Technologie setzen wollen, um langfristig Vorteile in der Umsetzung ihrer Geschäfts- und Wertschöpfungsprozesse zu generieren. Im Folgenden wird aufgezeigt, ob dies schon so ist und wo sich Ansatzpunkte für eine IT-Security-Strategie finden.

2 IST-Situation in deutschen Unternehmen

Nachholbedarf findet sich allerorten, wie jüngste Meldungen über ungesicherte Industrie-steuerungen, über die via Internet zugriffen werden kann, belegen.[1] Zur Konfiguration laufen Webserver auf den Embedded-Devices, deren rudimentäre Sicherheitsmaßnahmen (Passwort-abfrage) aufgrund von fehlenden Updates leicht zu umgehen sind. Dabei ist der Grund für die Sicherheitslücke zum einen darin zu sehen, dass z. B. serielle Schnittstellen an das Internet angebunden werden, die eigentlich nur für einen lokalen Zugriff vorgesehen waren und dementsprechend vor allem durch das Gebäude und die Räumlichkeiten abgesichert sind/waren, in den sie sich befinden. Zum anderen wird einfach auf sichere Kommunikationskanäle wie Virtual Private Networks (VPN) verzichtet, die den unbefugten Zugriff unterbinden würden.

Während vielerorts die Büromitarbeiter im Homeoffice also ganz vorbildlich ausschließlich per VPN auf das Unternehmensnetzwerk zugreifen, hängen Steuergeräte häufig relativ ungesichert im Internet – Zugriff kann praktisch jeder mit minimalem Aufwand erlangen. Hier ließe sich durch einfache Maßnahmen, wie sichere Authentifizierung an der Web-Konfiguration (sofern dies möglich ist) und Tunnelung über VPN, die Sicherheit auf ein gutes Niveau bringen. Die dafür notwendigen Techniken sind seit Langem vorhanden und erprobt.

Bei standortübergreifender Vernetzung bedürfen die Zugangspunkte bzw. Schnittstellen zwischen Unternehmens-LAN und Internet besonderer Absicherung. Zum einen müssen die Kommunikation

1 Siehe z. B. Louis-F. Stahl: „Gefahr im Kraftwerk. Industrieanlagen schutzlos im Internet“. c’t Magazin für Computertechnik 11/2013, S. 78–82.

Tel.: +49-(0)561-8109-0

bzw. der Datenverkehr im Internet über VPN abgesichert werden und zum anderen müssen die dahinterliegenden unternehmensinternen Netzwerke geschützt werden. Aber nicht nur auf der Infrastrukturebene muss an Absicherung gedacht werden, auch z. B. Systeme für Video Conferencing können aufgrund von Sicherheitslücken oder Fehlkonfigurationen plötzlich aus dem World Wide Web erreichbar sein.

Dass das Thema IT-Security an Bedeutung zunimmt, zeigen auch die Angaben der regelmäßig von techconsult befragten Unternehmen zu ihren Investitionen in den letzten Jahren. Es lässt sich eine kontinuierliche Steigerung in den Ausgaben für IT-Security feststellen, die sich im Bereich von 5–7 Prozent pro Jahr bewegt. Die größeren Unternehmen erhöhen ihre Investitionen dabei etwas stärker, die kleinen Unternehmen tendenziell etwas weniger stark (vgl. Abbildung 1).

IT-Security-Spendings (Mio. Euro)

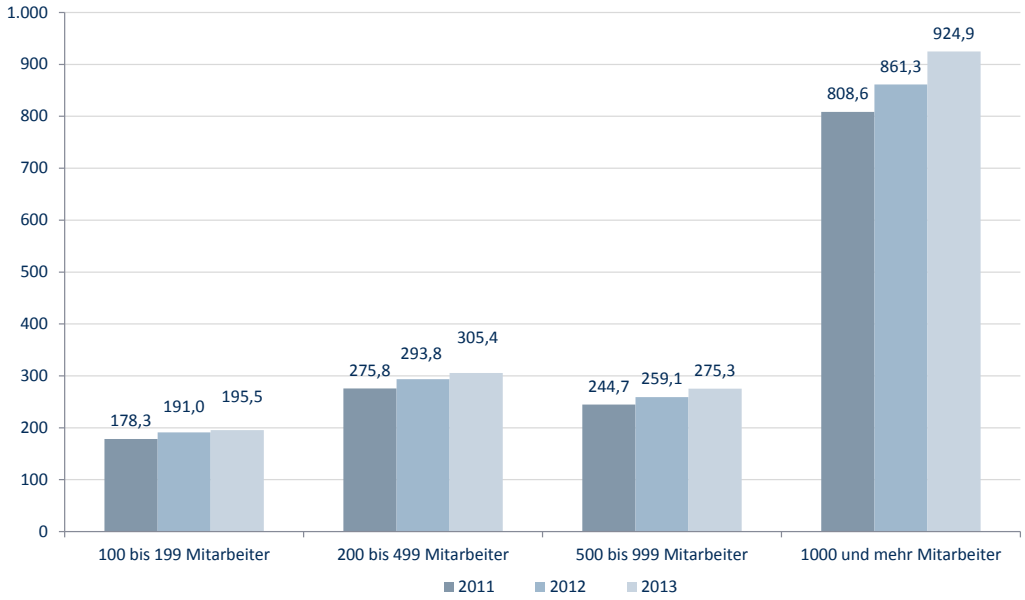


Abbildung 1: Ausgaben für IT-Security in den letzten Jahren

2.1 Status quo der IT-Sicherheit und IT-Security-Strategie

Dass es Nachholbedarf gibt, heißt jedoch nicht, dass sich Unternehmen der Gefahr nicht bewusst wären. In von techconsult befragten mittelständischen Unternehmen mit 20 bis 1.999 Mitarbeitern bereitet vor allem die Angst vor Fehlverhalten und leichtfertigem Umgang der Mitarbeiter mit Daten Sorgen, sowie die Angst, dass Schadsoftware (Viren, Trojaner) in das Unternehmen eingeschleppt wird und den Betriebsablauf stören könnte. An dritter Stelle steht das Risiko des Ausfalls von IT-Infrastruktur. Nur sehr wenige Unternehmen sehen sich keinen Risiken ausgesetzt (vgl. Abbildung 2).

Welchen Risiken sehen Sie sich und Ihre IT aktuell ausgesetzt?

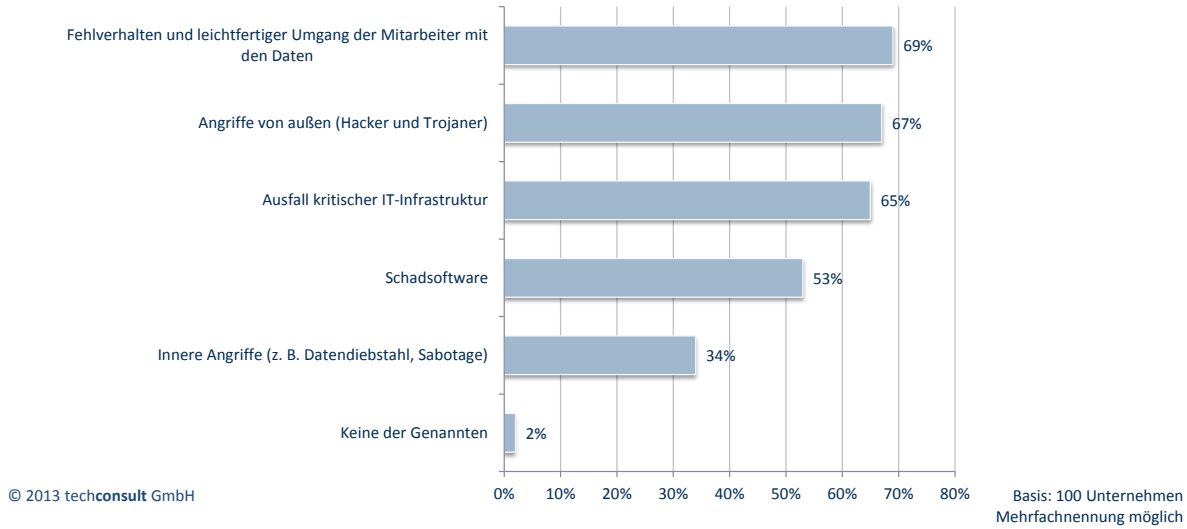


Abbildung 2: Risiken, denen sich Unternehmen ausgesetzt sehen

Daher greifen die meisten mittelständischen Unternehmen auf zusätzliche Maßnahmen zurück, um ihre IT-Infrastruktur abzusichern. Dies sind zumeist Software-Lösungen, die eine sichere Hardware-Basis nicht ersetzen können, bei einem Zwischenfall (Hacker-Angriff, Trojaner-Befall etc.) aber Möglichkeiten bieten, diesen zunächst einmal zu erkennen und dann im besten Fall abzuwenden bzw. zu beseitigen. Am häufigsten kommt hier die zentrale Firewall zum Einsatz (80 Prozent). Eng dahinter folgen zentrale Antivirenlösungen und Spamfilter, die zum Einsatz kommen. Noch fast zwei Drittel der mittelständischen Unternehmen setzen auf clientseitige Antivirenlösungen. Nur knapp über 40 Prozent betreibt Monitoring und Logging, um Hinweise auf eventuelle Sicherheitsprobleme zu erhalten. Umfassende und integrierte Systeme für Security Information and Event Management (SIEM), Intrusion Detection Systeme (IDS) und Unified Threat Management kommen bei nicht mal einem Viertel der Befragten zum Einsatz (vgl. Abbildung 3).

Wie sichern Sie derzeit Ihre IT-Infrastruktur?

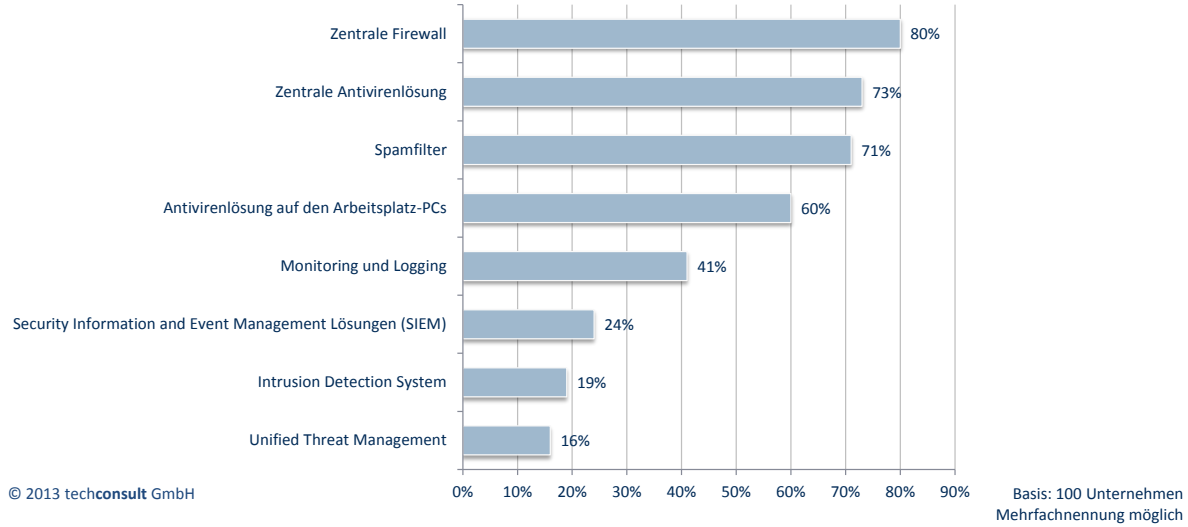
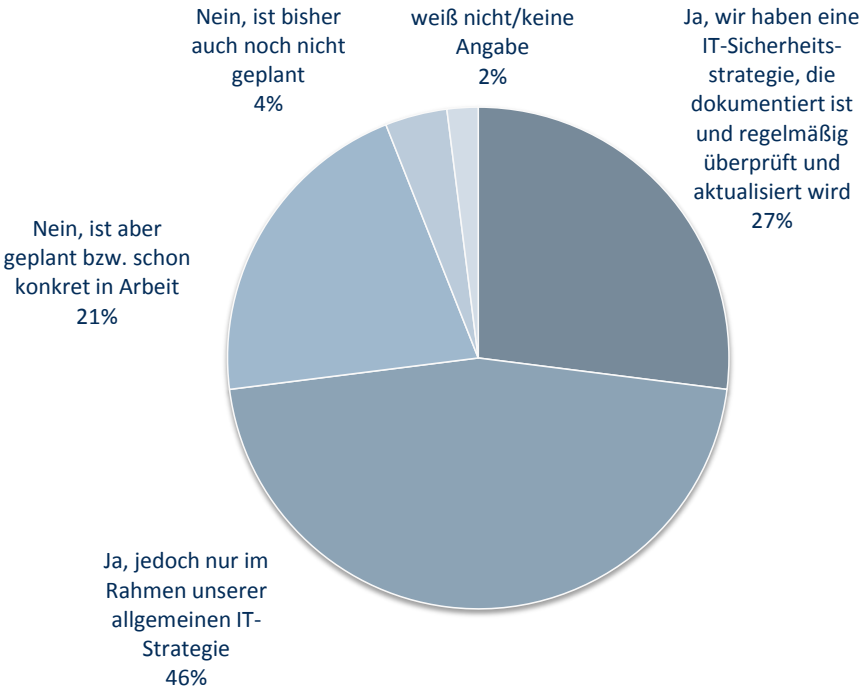


Abbildung 3: Additive Sicherungsmaßnahmen IT-Infrastruktur

Bezüglich der IT-Security-Strategie lässt sich feststellen, dass zusammengenommen fast drei Viertel der befragten Mittelständler eine IT-Security-Strategie haben. Bei den meisten Unternehmen (46 Prozent) ist diese jedoch nur im Rahmen einer allgemeinen IT-Strategie definiert. Nur bei 27 Prozent ist sie eigenständig, ist dokumentiert und wird regelmäßig überprüft und aktualisiert.

Bei 21 Prozent der befragten Unternehmen gibt es zwar noch keine IT-Security-Strategie, sie ist aber schon konkret in Planung. Nur 4 Prozent gaben an, dass sie weder eine IT-Security-Strategie haben noch eine solche in Planung ist.

Gibt es in Ihrem Unternehmen eine IT-Security Strategie und wie sieht diese aus?



Basis: 100 Unternehmen

Abbildung 4: IT-Security-Strategie

Inhaltlich kann die IT-Security-Strategie ganz unterschiedlich ausgeprägt sein. Was die Anschaffung neuer Hardware betrifft, versuchen die meisten Anwenderunternehmen hauptsächlich durch additive Sicherheitsmaßnahmen (Virenscanner, Firewalls) ihre IT-Infrastruktur abzusichern (68 Prozent). Diese Strategie in der Kombination mit der Anschaffung sicherer Hardware verfolgen 56 Prozent der Befragten. Knapp etwas weniger als die Hälfte der befragten mittelständischen Unternehmen setzt auch schon bei der Anschaffung an und legt den Fokus auf sichere Hardware, Sicherheitsstandards und Zertifizierungen (48 Prozent). Eine darüber hinausgehende eigene Analyse (Sicherheits-Audits etc.) führen nur 29 Prozent der Befragten durch. Für 17 Prozent ist die werkseitige Sicherheit ausreichend, für lediglich 3 Prozent spielt Sicherheit bei der Anschaffung keine Rolle (vgl. Abbildung 5).

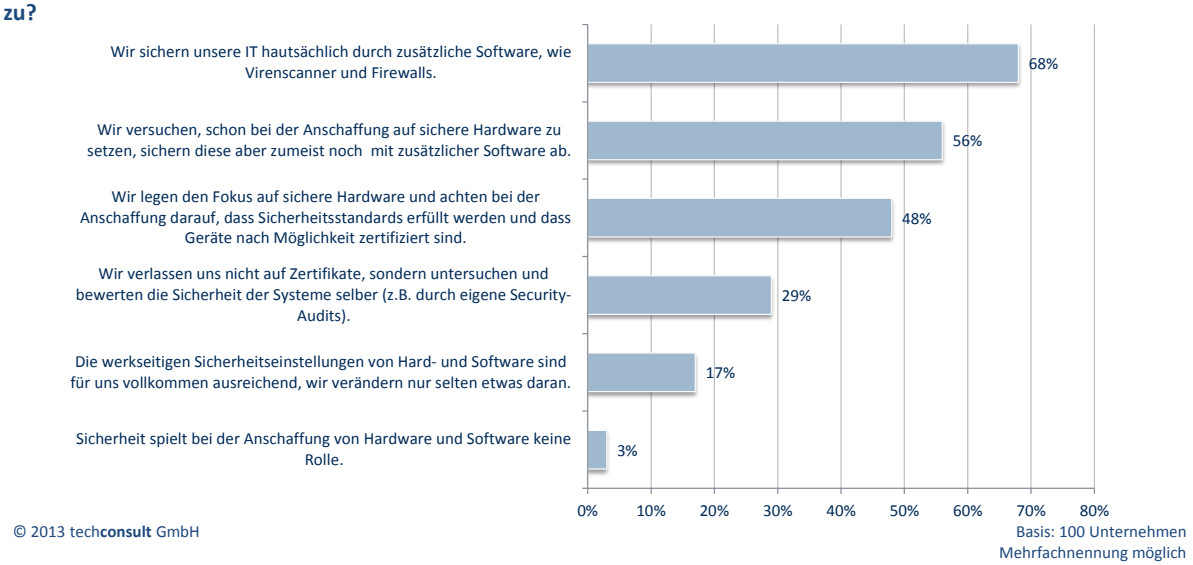


Abbildung 5: IT-Security-Strategie in Bezug auf Hardware-Anschaffung

Nach der Neuanschaffung der Hardware ist natürlich auch für den laufenden Betrieb sicherzustellen, dass die IT-Infrastruktur abgesichert ist. Dazu sind regelmäßige Updates notwendig, die Fehler beheben und Sicherheitslücken schließen. Gut drei Viertel der befragten Mittelständler aktualisiert die eingesetzte Software regelmäßig. 42 Prozent warten darauf, dass Hersteller Sicherheitsupdates veröffentlichen. Jeweils ungefähr ein Drittel verfolgt auch Security Bulletins und hilft sich mit Workarounds oder Patches, um bekanntgewordene Sicherheitslücken zu schließen. Nur 4 Prozent geben an, dass Systeme überhaupt nicht aktualisiert werden – tendenziell waren diese vereinzelten Nennungen eher bei großen Unternehmen zu finden. Tendenziell ist bei größeren Unternehmen aber auch eine größere Aktivität zu verzeichnen, was eigene Maßnahmen unabhängig vom Hersteller betrifft.

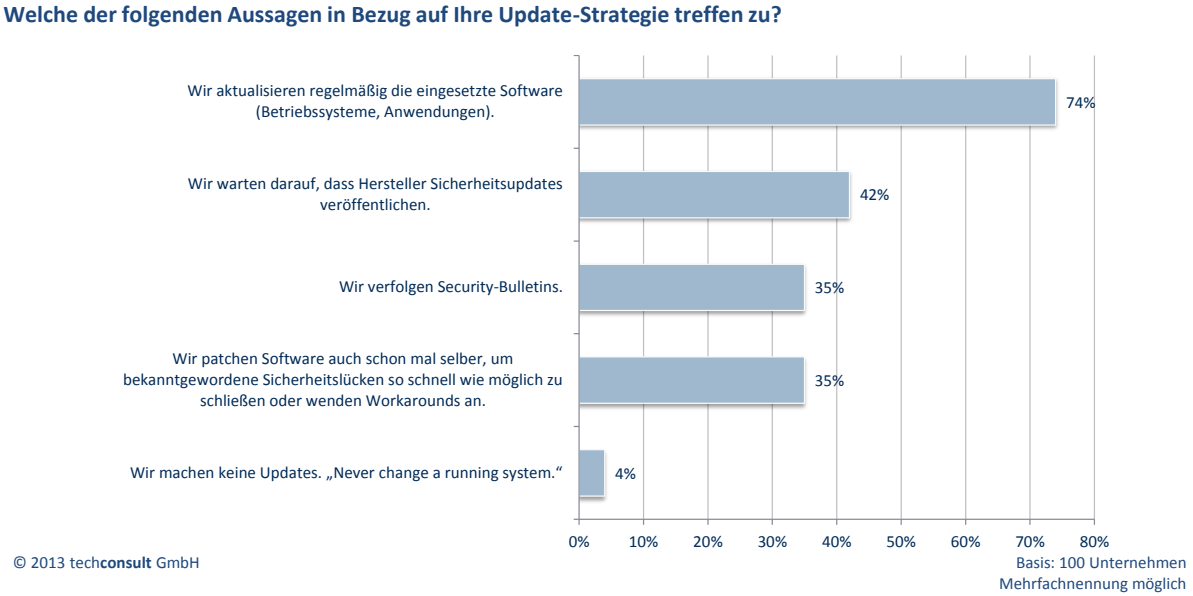


Abbildung 6: IT-Security-Strategie bezüglich Software-Updates

2.2 Elemente einer umfassenden IT-Security-Strategie

Einzelne Maßnahmen zur Absicherung der eigenen IT-Infrastruktur lassen sich in drei Teilstrategien unterteilen, die im Idealfall zusammengenommen eine umfassende IT-Security-Strategie bilden:

Der *passive* Anteil einer IT-Security-Strategie beinhaltet, dass regelmäßig Sicherheitsupdates der Hersteller eingespielt werden. Der Admin muss hier zwar in gewissem Sinne auch aktiv werden, diese Maßnahmen sind aber deshalb als eher passiv einzustufen, weil hier vor allem der Hersteller aktiv wird und die Verfügbarkeit der Updates zumeist vom Gerät gemeldet wird. Der einzige aktive Teil auf Seiten der IT-Abteilung ist die Installation anzustoßen.

Bei einer *aktiv-reaktiven Sicherheitsstrategie* werden Maßnahmen ergriffen, um Bedrohungen abzuwenden. Dabei werden die Angriffspunkte nicht unbedingt entfernt, sondern hauptsächlich durch additive Maßnahmen abgesichert. So werden Virenscanner und Firewalls genutzt, um zukünftige Fälle auszuschließen. Dazu kann auch gehören, dass Security-Bulletins verfolgt werden, um so möglichst frühzeitig auf Sicherheitsprobleme aufmerksam zu werden und Updates, Patches und Bugfixes beziehen zu können.

Als *proaktiv-präventive Sicherheitsstrategie* kann eine Strategie beschrieben werden, die schon bei der Planung und Anschaffung ansetzt. Dabei wird z. B. von vornherein auf Hardware gesetzt, die bestimmte definierte Kriterien erfüllen, also etwa von einer (hersteller-) neutralen Stelle (BSI, TÜV etc.) zertifiziert wurde. Weiterhin umfasst der proaktive Bereich die selbstständige Suche nach

Fehlern in der eingesetzten Hard- und Software sowie Konfigurationen. Dies umfasst z. B. unstandardisierte Tests, wie einfachen Portscans und kann dann je nach eigener (Sicherheits-) Anforderung auch ein eigener Audit-Prozess sein, der die Einhaltung der Richtlinien und Maßnahmen überprüft. Darüber hinaus sind hier auch eigene Beiträge zum Bugreporting und der Entwicklung von Patches für die eingesetzte Software zu sehen. Dieses Idealbild kann natürlich nur in begrenztem Maße umgesetzt werden, schließlich bedeutet dies auch einen nicht geringen Aufwand, der Mitarbeiter bindet. Außerdem besteht diese Möglichkeit der aktiven Beteiligung nicht bei jeder Software, sondern hauptsächlich dort, wo Sicherheitslücken offen diskutiert werden, also z. B. bei Open-Source-lizensierter Software.

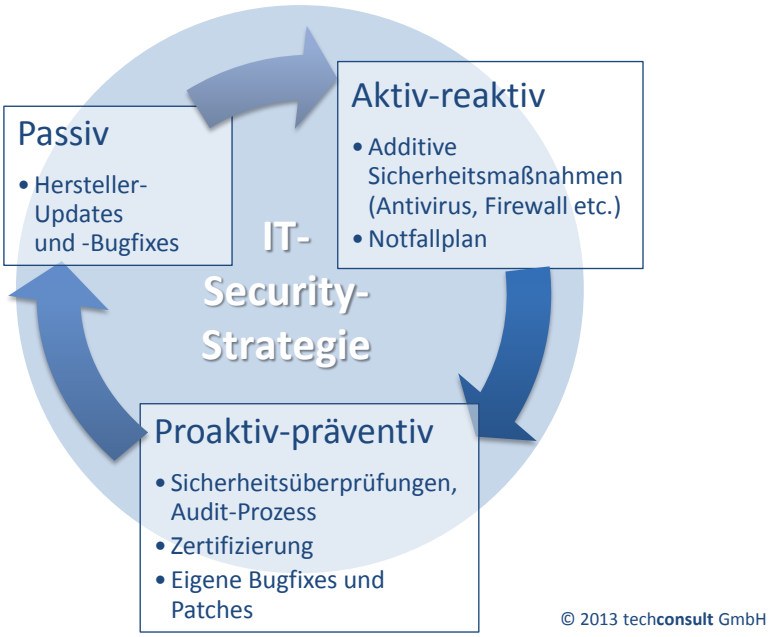


Abbildung 7: Teilstrategien einer IT-Security-Strategie

Nur die wenigsten Unternehmen können die beschriebenen Teilbereiche jeweils umfassend umsetzen, es lohnt sich aber für jedes Unternehmen, für jeden der einzelnen Bereiche zu prüfen, welche Maßnahmen möglich sind. Einseitige Sicherheitsstrategien sind kontraproduktiv: Es reicht nämlich nicht, nur zu reagieren, wenn es einen akuten Problemfall gibt, sondern es sollten schon im Vorfeld präventive Maßnahmen ergriffen worden sein. Dann kann schon die Wahrscheinlichkeit für das Auftreten sicherheitskritischer Zwischenfälle gesenkt und so deren Anzahl reduziert werden. Trotzdem muss ein Notfallplan für eine angemessene Reaktion vorhanden sein, um ggf. geschäftskritische Anwendungen schnell wieder verfügbar machen zu können und die Ausfallzeiten zu minimieren.

3 Ausgangs- und Ansatzpunkte für eine IT-Security-Strategie

3.1 IT-Security als Querschnittsthema

Da der IT-Unterstützungsgrad ein für den Erfolg einer Abteilung oder eines Prozesses und damit insgesamt für den Unternehmenserfolg immer wichtiger werdendes Kriterium ist, erlangt auch das Thema IT-Security als abteilungsübergreifendes Querschnittsthema immer mehr an Bedeutung. Sowohl in den einzelnen Abteilungen als auch dann in der Summe für das gesamte Unternehmen ist diese umzusetzen, um Unternehmensbereiche bzw. Abteilungen und Prozesse effizient aufzustellen sowie Schäden, z. B. durch Ausfall, Datenverlust oder gar Datendiebstahl zu vermeiden. Auch auf der Ebene verschiedener Trend-Themen lässt sich IT-Security als Querschnittsthema identifizieren. Dies sind z. B. die Themen Mobility und Consumerization of IT (CoIT), Video Conferencing, Cloud Computing sowie Industrie 4.0.

Der zunehmende Mobility-Trend und CoIT bringen mit sich, dass verstärkt auf Funktechnologien gesetzt wird. Diese wiederum erfordern Absicherungsmaßnahmen, wie sichere Authentifizierung und Verschlüsselung der Kommunikation. Das Thema CoIT stellt für Unternehmen gewissermaßen eine Möglichkeit dar, für ihre Mitarbeiter das Nützliche mit dem Angenehmen zu verbinden: Die Mitarbeiter sind es von ihren privaten Endgeräten gewohnt, ein ansprechendes User-Interface, Haptik usw. geboten zu bekommen, die dem Business-PC in der Regel fehlt. Für Unternehmen kann es daher durchaus lohnenswert sein, den Mitarbeitern den Einsatz ihrer privaten Endgeräte zu gestatten und diese dafür in einem gewissen Umfang zu entschädigen.

Auf der Schattenseite dieses Trends muss jedoch auch in Rechnung gestellt werden, dass sich der Administrationsaufwand aufgrund der Gerätevielfalt und dem Fehlen von z. B. Remote-Management-Funktionen auch erhöht. Auch bedürfen die Sicherheitsmaßnahmen eines höheren Aufwands, um der Heterogenität der Endgeräte und den unterschiedlichen Möglichkeiten und Beschränkungen bei der Umsetzung einer IT-Sicherheits-Strategie gerecht zu werden. Die Zunahme von „Bring Your Own“ bringt auch verstärkte Security-Maßnahmen mit sich, um den Ängsten vor Datenverlust, Datenklau etc. zu begegnen, die die Einbindung der Geräte ins Unternehmensnetzwerk mit sich bringt.

Aktuelle Aufdeckungen von schwerwiegenden Sicherheitsproblemen bei der Nutzung von Video-Conferencing-Lösungen zeigen, wie kritisch die Lage ist: Hier fließen u. U. unbemerkt auf höchster Ebene unternehmensinterne Daten ab. Der Schaden, der dabei entsteht, kann in den meisten Fällen gar nicht beziffert werden. Dabei besteht durch die Umstellung der gesamten Telefonie auf die IP-

Plattform die Möglichkeit, diese relativ einfach per VPN abzusichern – dies war im ISDN-Zeitalter nur mit hohem Aufwand und hohen Kosten umzusetzen.

Auch die zunehmende Cloud-Nutzung im Mittelstand bringt das Thema IT-Security auf die Tagesordnung. Nicht nur E-Mail, sondern auch Cloud-Lösungen wie z. B. Customer Relationship Management (CRM) müssen besonders abgesichert sein. Liegen diese in der Public Cloud, kann die Absicherung dort zwar von Seiten des Cloud-Anbieters gegeben sein, Angriffsfläche und Einfallstore kann die IT-Infrastruktur im Unternehmen dann trotzdem bieten. Wichtig ist außerdem, dass nicht nur die Datenspeicherung in der Cloud sondern auch die Verbindung in die Cloud abgesichert ist, z. B. durch einen VPN-Tunnel. Darüber hinaus gilt es auch, sich rechtlich abzusichern, was durch Merkmale wie Server-Standort in Deutschland unterstützt wird.

Die unter dem Schlagwort „Industrie 4.0“ zusammengefasste Entwicklung der zunehmenden Vernetzung von Maschinen/Anlagen, die auf Computer-Technologien basiert, bedeutet vor allem, dass das Zusammenspiel von Maschinen/Anlagen nicht mehr individuell in Elektronik realisiert ist, sondern mit Hilfe von Informationstechnologie. Dadurch ergibt sich ein riesiges Vernetzungspotenzial, weil prinzipiell jede Anlage mit jeder anderen vernetzt werden kann. Darüber hinaus werden dieselben Vernetzungstechnologien (Ethernet, TCP/IP etc.) wie auf IT-Seite genutzt, was die Anbindung der Anlagen an Intranet und Internet erlaubt und so die Integration in IT-gestützte Prozess- und Analyse-Tools ermöglicht. Dabei laufen in Echtzeit Daten zusammen, deren ständige Überwachung z. B. hochdynamische Produktionsprozesse erlaubt, die die gesamte Wertschöpfungskette vom Auftrag bis zur Auslieferung (und darüber hinaus, z. B. Service) integrieren und die interaktiv und automatisiert justiert werden können.

Die Konsequenz in Bezug auf die IT-Sicherheit ist offensichtlich: Je interaktiver und vernetzter die Systeme, desto größer und weitreichender können auch Schäden sein, die durch Ausfälle entstehen können.

3.2 Bewusstsein schärfen und Strategien finden

Im Mittelstand fehlt häufig immer noch das Bewusstsein für die Notwendigkeit von IT-Security-Maßnahmen und -Strategien. Es lässt sich jedoch im Zuge des zunehmenden Einsatzgrades von Cloud-Lösungen auch im Mittelstand die Tendenz erkennen, dass zum einen das Bewusstsein steigt und zum anderen auch vermehrt professionelle Lösungen in Form von Security-as-a-Service bezogen

werden: Im quartalsweise erhobenen IT-Cloud-Index Mittelstand[2] gaben 35 Prozent der befragten mittelständischen Unternehmen an, in den letzten drei Monaten Security-Lösungen bzw. Endpoint-Protection als Software-as-a-Sevice bezogen zu haben.

Security-as-a-Service ist gerade für den Mittelstand ein guter Ansatz, weil hier oft das IT-Know how fehlt und je nach Branche auch die IT-Affinität nicht so stark ausgeprägt ist. Trotzdem müssen dann wiederum die Zugangspunkte gut abgesichert sein. Consumer-Hardware bietet in der Regel kein ausreichendes Sicherheitsniveau und kann die IT-Sicherheit gefährden, die mit Security-as-a-Service angestrebt wird.

Dies kann sich dann auch direkt auf der betriebswirtschaftlichen Seite widerspiegeln: Eine Betriebsausfallversicherung kann bei mangelnder IT-Sicherheit teuer werden. Zertifizierte Hardware bietet hier einen guten Ausgangspunkt: Durch sie kann im Schadensfall zumindest nachgewiesen werden, dass eine gesunde, d. h. angemessene Sorgfalt an den Tag gelegt wurde und nicht grob fahrlässig auf eine grundlegende IT-Sicherheit verzichtet wurde.

Für Zulieferbetriebe als Auftragnehmer kann außerdem von Bedeutung sein, dass Compliance-Anforderungen von Kunden berücksichtigt und vertragliche Zusicherungen eingehalten werden müssen. Hier kann der Einsatz zertifizierter Hardware eine Vertrauensbasis in Bezug auf IT-Security schaffen.

Auch wenn es um Neuinvestitionen geht, muss an einen Zusammenhang von IT-Security und betriebswirtschaftlicher Ebene gedacht werden, denn Kreditkonditionen können mitunter von der mit Basel II geforderten IT-Sicherheit abhängig gemacht werden. Im Rahmen von Basel II werden IT-bedingte Risiken in Form der Operationalen Risiken mit in die Risikobewertung in Vorfeld einer Kreditvergabe einbezogen. In diesem Zusammenhang wird dann zertifizierte Hardware kein hinreichendes Kriterium sein, sehr wohl aber ein guter Ausgangspunkt und Teil der geforderten Maßnahmen zur Sicherstellung von IT-Security.

In Anwenderbefragungen, die von techconsult durchgeführten wurden, ließ sich immer wieder feststellen, dass ab dem gehobenen Mittelstand eigentlich alle Unternehmen Anwendungen nutzen, die sie als geschäftskritisch einstufen. Kommt es zum Ausfall, können zwar in den meisten Fällen ein

2 In dem von techconsult erhobenen IT-Cloud-Index Mittelstand werden vierteljährlich ca. 200 Unternehmen des deutschen Mittelstandes mit 20 bis 1.999 Mitarbeitern zu ihrem derzeitigen und zukünftigen Cloud-Einsatz befragt. Darüber hinaus steht allen Interessierten unter http://www.it-cloud-index.de der kostenlose Cloud-User-Check zur Verfügung, mit dem die eigene Cloud-Nutzung bewertet werden kann.

Tel.: +49-(0)561-8109-0

paar Stunden verkraftet werden, trotzdem fallen für diese Ausfallzeiten Kosten an. Auf das Jahr und die gesamte deutsche Unternehmenslandschaft hochgerechnet, gelangt man schnell in den Milliarden-Euro-Bereich.

3.3 Auswahlkriterium „Made in Germany“

„Made in Germany“ gewinnt als Auswahlkriterium bei der Anschaffung von IT-Infrastruktur-Komponenten zusehends an Bedeutung. Dabei geht es nicht zentral um Verarbeitungsqualität, wofür das Label sonst meist steht, sondern um Vertrauenswürdigkeit von Herstellern und Einhaltung von rechtlichen Rahmenbedingungen in Deutschland. Zum einen wird hier häufig Industriespionage als Bedrohung gesehen, aber auch die Überwachung von Kommunikation durch z. B. Regierungs-behörden, die durch Backdoors in den Produkten ermöglicht werden.

Einheimische Hersteller unterliegen den hiesigen gesetzlichen Vorgaben, die vor solchen Praktiken schützen sollen und richten auch darauf ihren Entwicklungsprozess aus, in den die Entwicklungs-arbeit im besten Fall nach hierzulande gültigen Standards in ein Produkt einfließt. Es liegt natürlich für einen deutschen Hersteller näher, sich auf die Sicherheitsstandards des deutschen Marktes einzulassen und z. B. die Empfehlungen des BSI in seinen Produkten umzusetzen; nicht zuletzt auch darum, weil er damit auf das Vertrauen seiner Kunden hoffen kann.

3.4 Zertifikate als Siegel und Garantie für geprüfte Sicherheit

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist als herstellerunabhängige Organisation eine Instanz, die mit dafür sorgt, das Bewusstsein für IT-Sicherheit zu schaffen. Hier werden zum einen Kriterien entwickelt, um IT-Produkte mittels einheitlicher Verfahren auf ihre Sicherheitseigenschaften zu untersuchen und zu bewerten. Das BSI hat dazu einige Prüfstellen ernannt, die diese Dienstleistung anbieten, z. B. für Hersteller von IT-Hardware. Zum anderen hat das BSI die Aufgabe, den Weg Deutschlands in die Informationsgesellschaft zu begleiten und durch Expertise und Unabhängigkeit die damit verbundenen Risiken zu minimieren.

Die nach BSI-Kriterien zertifizierte Hardware bietet somit mit die bestmögliche Umsetzung von Richtlinien aus deutschen Gesetzen, wie z. B. dem Bundesdatenschutzgesetz, bis hin zu internationalen Standards, wie der ISO-Norm 27001 oder den sogenannten „Common Criteria“ (ISO 15408). Die Common Criteria heben sich darüber hinaus als Standard hervor, der international per Abkommen in 26 Ländern von Bedeutung ist. In 16 dieser Länder werden Zertifizierungen

vorgenommen[3], weitere zehn erkennen die Common Criteria an[4]. Die Zertifizierung von Systemen und Komponenten nach Common Criteria wird in Deutschland bis zur Stufe EAL 4+ vom BSI erteilt, der höchsten wechselseitig international anerkannten Zertifizierungsstufe. Dazu lassen Hersteller ihre Produkte in vom BSI anerkannten Prüfstellen in einem aufwendigen, in der Regel mehrjährigen Verfahren prüfen und – falls die Bewertung positiv verläuft – für die Dauer von drei Jahren zertifizieren. Die Begutachtungsphase umfasst dabei Systembegutachtungen und Fachbegutachtungen zur Bewertung der Sicherheit und Vertrauenswürdigkeit der zu evaluierenden Systeme und Komponenten, die Testverfahren wie z. B. aufwändige Penetrations- und Vulnerability-Tests beinhalten. Die herstellerunabhängige Entwicklung der Prüfkriterien bietet somit gerade mittelständischen Anwenderunternehmen einen Mehrwert, den man in der Regel selbst nicht erbringen kann – aus Gründen des fehlenden Know-hows oder aufgrund mangelnder Ressourcen.

3 Australien, Deutschland, Frankreich, Großbritannien, Italien, Japan, Kanada, Malaysia, Neuseeland, Niederlande, Norwegen, Südkorea, Spanien, Schweden, Türkei und USA.

4 Dänemark, Finnland, Griechenland, Indien, Israel, Österreich, Pakistan, Singapur, Tschechische Republik und Ungarn.

Tel.: +49-(0)561-8109-0

4 Fazit

Die Etablierung einer sicheren IT-Infrastruktur ist eine der Aufgaben des CIOs und seiner IT-Mitarbeiter, die letzten Endes sicherstellen müssen, dass das Unternehmen und seine Computer, Daten, Anlagen, Steuerungen usw. vor unbefugtem Zugriff geschützt sind. Oft ist sie aber auch eine strategische Entscheidung von oben: Als Investition in eine solide Basis – zum Beispiel Infrastrukturlösungen mit BSI-Sicherheitszertifizierung – statt in vermeintlich günstigere Infrastruktur, die im Nachhinein nur teuer und zumeist nur suboptimal abgesichert werden kann.

Notwendig ist auch die Sensibilisierung der IT-Mitarbeiter für eine IT-Security-Strategie und die Sicherstellung ihrer Umsetzung. Langfristig sollte sich der Gedanke „Security by Design“ (von Grund auf eingeplant), also ausgehend von der IT-Security-Strategie für die IT-Infrastruktur durchsetzt, statt nur nachträglich ein Strategie oben aufzusetzen. Dies ist zielführender, als durch additive Sicherheitslösungen zu versuchen, die Probleme in der Infrastruktur-Basis zu lösen. Denn dadurch verschwinden vorhandene Sicherheitslücken nicht, sondern sind bestenfalls nur nicht mehr direkt sichtbar. Gewissermaßen gilt derselbe Leitsatz, der auch bei der Absicherung eines Hauses beherzigt werden sollte: Wenn die Kellertür offensteht, helfen auch die Gitter im Erdgeschoss nicht.

Zum Status Quo der aktuellen IT-Security-Maßnahmen und -Strategien in deutschen Unternehmen lässt sich abschließend noch feststellen, dass sich etwas mehr als die Hälfte der Mittelständler angemessen geschützt sehen. Sogar für die Zukunft gerüstet sehen sich weitere 15 Prozent. Bei einem Viertel reicht es gerade so aus, jeder Zwanzigste ist der Meinung, dass dringend etwas getan werden muss (vgl. Abbildung 8).

Insbesondere für den Großteil derer, die sich jetzt angemessen geschützt fühlen, bedeutet dies, dass sie ihre IT-Security-Strategie und die damit verbundenen -Maßnahmen ständig überprüfen und anpassen müssen, um neuen Bedrohungen gewachsen zu sein. Angesichts der ständig bekannt werdenden Sicherheitslücken und Zero-Day-Exploits, die diese ausnutzen, wird deutlich, dass hier kaum Zeit ist, sich auszuruhen, sondern man eher gefordert ist, IT-Security-Maßnahmen und -Strategien ständig weiter zu entwickeln. Nicht zuletzt muss natürlich auch für die Selbsteinschätzung die Möglichkeit in Betracht gezogen werden, dass man falsch liegt und gar nicht so gut aufgestellt ist, wie es scheint. Hier helfen regelmäßige Überprüfungen und Security-Audits, zu einer realistischen Einschätzung der eigenen Lage zu kommen.

Tel.: +49-(0)561-8109-0

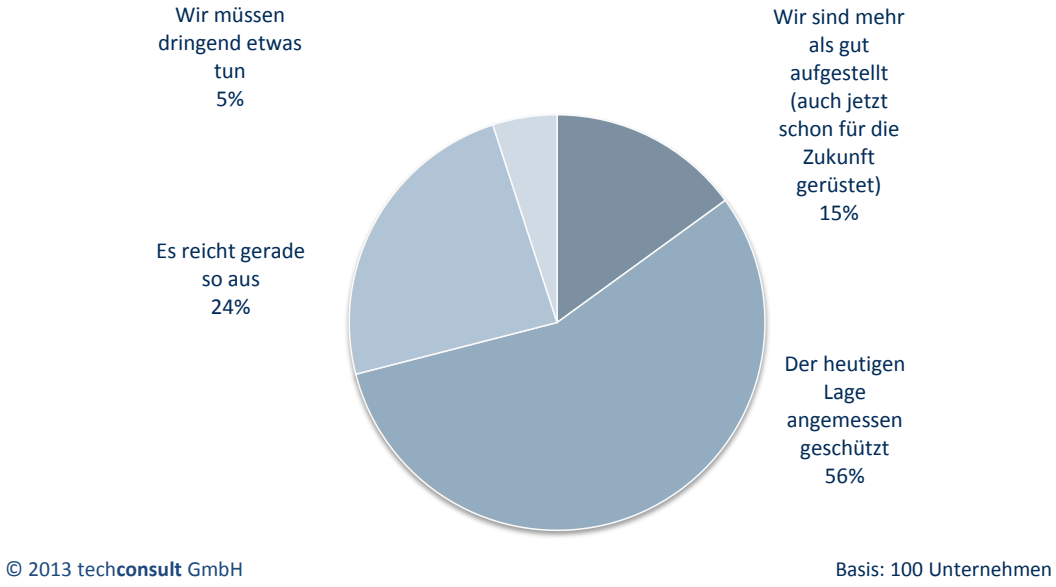
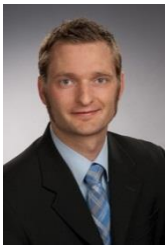


Abbildung 8: Einschätzung der eigenen IT-Security-Maßnahmen

Für die, deren Maßnahmen gerade noch so ausreichen, und die, die dringenden Handlungsbedarf sehen, ist es nur eine Frage der Zeit, wann der nächste Zwischenfall zu einem wohlmöglich größeren Ausfall führt, wenn hier nicht mit strategischer Planung und nötigenfalls Investitionen ein höheres Niveau bezüglich IT-Security anvisiert wird.

Für Zukunftsthemen wie Industrie 4.0, die jetzt gerade aktuell werden, zeigt diese Selbst-einschätzung, dass man in den meisten Fällen die eigene IT-Sicherheit einen großen Schritt nach vorn wird bringen müssen, will man in diesen Bereich vorstoßen.

Autor:



Henrik Groß
– Research Analyst –

techconsult GmbH
Am Platz der Deutschen Einheit
Leipziger Straße 35–37
34125 Kassel

Tel.: +49-(0)561-8109-0
Fax: +49-(0)561-8109-101
Web: http://www.techconsult.de

Weitere Informationen für Journalisten und PR:

Yildiz Cinar
– Leiterin Public Relations –
Tel.: +49-(0)561-8109-132
E-Mail: yildiz.cinar@techconsult.de

Über techconsult

Die techconsult GmbH gehört zu den führenden Marktforschungs- und Marketingconsulting-Unternehmen in Zentraleuropa mit Fokus auf die Informations- und Kommunikationstechnik-Branche. Zum Unternehmen gehören engagierte Wissenschaftler aus den Disziplinen Technologie-Marketing, Marktforschung und Informationstechnik. techconsult gehört seit Juni 2012 zur Heise Medien Gruppe. Mehr Informationen finden Sie im Internet unter http://www.techconsult.de.

Dieses Market Paper wurde unterstützt von LANCOM Systems.