techconsult
The IT Market Analysts

2. Bericht zur Studie „Security-Bilanz Deutschland“

Pain-Points der Umsetzung von IT-Sicherheitsmaßnahmen

-- Kurzbericht * --

1. Bericht zur Studie „Security-Bilanz Deutschland“

Der Status Quo der IT-Sicherheit im deutschen Mittelstand

SecurityBilanz

EINE STUDIE ZUR
IT- UND INFORMATIONSSICHERHEIT
KLEINER UND MITTELSTÄNDISCHER UNTERNEHMEN
IN DEUTSCHLAND

techconsult The IT Market Analysts | Heise | SecurityConsulter

Studienbeirat:

BITKOM | Bundesamt für Sicherheit in der Informationstechnik | heise Security | TeleTrusT Pioneers in IT security. | wecon.it-consulting »we.secure-your.it«

Sponsorenpartner:

FORTINET | mesh | Microsoft | T | baramundi software AG | IBM | NCP SECURE COMMUNICATIONS | SOPHOS Security made simple. | NEXT GENERATION MANAGED SECURITY NETWORK BOX | brainloop | TREND MICRO

* Der Gesamtbericht zum Download:
www.Security-Bilanz.de

Inhalt

Copyright

Disclaimer

i. Status Quo der Umsetzung von IT- und Informationssicherheit

Die Studie Security Bilanz Deutschland hat sich zum Ziel gesetzt, einen umfassenden Blick auf IT- und Informationssicherheit in Unternehmen des deutschen Mittelstandes zu werfen. Dazu wurden Anfang 2014 über 500 Unternehmen mit 20 bis 1.999 Mitarbeitern befragt, wie sie selbst die IT- und Informationssicherheit in ihrem Unternehmen einschätzen. Die Perspektive folgt einem ganzheitlichen Ansatz, der nicht nur die technische Ebene in Form von IT-Konzepten, -Maßnahmen und -Lösungen in den Blick nimmt, sondern auch die organisatorische, rechtliche und strategische Ebene in mittelständischen Unternehmen mit einbezieht.

Der erste Studienbericht hat den Fokus auf Indices gelegt, die als übergeordnete Maßzahlen eine Gesamteinschätzung der aktuellen Sicherheits- sowie Gefährdungslage greifbar machen. Darüber hinaus dienen die Indices auch dem Vergleich, den das Self-Check-Tool *Security Consulter*[1] bietet, das techconsult in Zusammenarbeit mit Heise Security entwickelt hat und welches zur kostenfreien Nutzung jedem interessierten Unternehmen zur Verfügung steht (www.heise-consulter.de).

Erstes Studienfazit: trügerische Sicherheit

Das Fazit des ersten Studienberichts zur IT- und Informationssicherheit: Der Mittelstand fühlt sich relativ sicher. Gegenüber der wahrgenommenen Gefährdung scheint das Sicherheitsniveau ausreichend zu sein. Die dabei erreichten Werte des Sicherheitsniveaus (Sicherheitsindex), im Mittel 58 von 100 Indexpunkten, zeigen jedoch auf, dass noch deutlich Luft nach oben bleibt, bevor von einer guten durchschnittlichen Umsetzung gesprochen werden kann. Hinzu kommt, dass der Sicherheitsvorsprung von 11 Indexpunkten zwischen Sicherheitsindex (58 Punkte) und Gefährdungsindex (46 Punkte) nur ein geringer Puffer ist, um auch für bisher unbekannte Gefahren gerüstet zu sein.

Im vorliegenden Bericht stehen nun nicht mehr die Indices selbst im Fokus, sondern die Umsetzung spezifischer Maßnahmen.

[1] Den Security Consulter finden Sie unter https://www.heise-consulter.de/

Hierzu wurde der Anteil der Unternehmen ermittelt, die ihre eigene Maßnahmenumsetzung in den abgefragten Handlungsbereichen als unzureichend einschätzen.

(subjektive) Relevanz aktueller Bedrohungsszenarien

In Kapitel 1 „Bedrohungsszenarien – (subjektive) Relevanz und Einschätzung des aktuellen Schutzes“ wird untersucht, von welchen Bedrohungensszenarien die größten Gefahren ausgehen- und an welchen Stellen die größten Umsetzungsdefizite von Maßnahmen, Lösungen und Konzepten der IT- und Informationssicherheit zu verorten sind. Hierbei handelt es sich nicht um objektive Fakten, sondern um die rein subjektive Sichtweise der Unternehmen. Doch gerade dieser subjektive Eindruck ist ein wichtiger Einflussfaktor im Entscheidungsprozess darüber, welche Maßnahmen und Lösungen im Unternehmen eingesetzt werden sollen. Je relevanter eine Bedrohung eingeschätzt wird, desto höher ist die Bereitschaft, entsprechende Gegenmaßnahmen zu ergreifen, umgekehrt, je weniger relevant eine spezifische Bedrohung erachtet wird, desto höher ist die Bereitschaft, ein vermeintlich geringes Risiko in Kauf zu nehmen.

Variation des Schutzniveaus in Geschäftsbereichen

Mit Kapitel 2, „Umsetzung von IT- und Informationssicherheit in Geschäftsbereichen“, rücken die einzelnen Funktionseinheiten der Unternehmen in den Fokus der Betrachtung. Wird IT- und Informationssicherheit unternehmensweit in gleicher Weise umgesetzt oder lassen sich Bereiche identifizieren, in denen größere Anstrengungen unternommen werden als in anderen? Unterschiedliche Umsetzungsgrade in einzelnen Bereichen bieten so auch Hinweise darauf, welche Daten in den Unternehmen als besonders schützenswert erachtet werden. Weiterhin liefern sie Anhaltspunkte, wie der Ausbau der IT- und Informationssicherheitsmaßnahmen effektiv vorangetrieben werden kann: Existieren unternehmensintern bereits Beispiele, die im Sinne der Best-Practice auch in anderen Unternehmensbereichen umgesetzt werden können?

Detailanalyse von Maßnahmen und Lösungen

Die Detailanalyse „Umsetzung von IT- und Informationssicherheit nach Handlungsfeldern“ ist Bestandteil des kompletten Berichts, der ihnen nach Registrierung für die Security-Bilanz Deutschland in Ihrem User-Center zum Download zur Verfügung steht.

Die Dateilauswertung umfasst die Auswertung der wichtigsten Maßnahmen und Lösungen zur IT- und Informationssicherheit im technischen, organisatorischen, rechtlichen und strategischen Handlungsfeld. Diese Detailbetrachtung liefert tiefe Einblicke zum Stand der Umsetzung von IT-Maßnahmen und dadurch auch zur Frage, ob die Unternehmen ihren eigenen Ansprüchen gerecht werden. Stimmen die Relevanzbewertung einzelner Bedrohungsszenarien mit bisher umgesetzten Schutzmaßnahmen überein oder werden einzelne Bedrohungen zwar als relevant erachtet, aber entsprechende Gegenmaßnahmen dennoch nicht ausreichend umgesetzt?

ii. Management Summary- Findings

BEDROHUNGSSZENARIEN – SUBJEKTIVE EINSCHÄTZUNG DER RELEVANZ

- Keines der genannten Bedrohungsszenarien wird von mehr als 40 Prozent aller befragten Unternehmen als relevant erachtet. Dies ist nicht nur der deutliche Beleg eines gering ausgeprägten Problembewusstseins, es dokumentiert vielmehr eine völlige Fehleinschätzung der aktuellen Bedrohungslage, sowie der Reichweite möglicher Konsequenzen erfolgreicher Cyber-Angriffe.
- Im Vergleich schreiben der Handel, öffentliche Verwaltungen, sowie Non-Profit-Unternehmen, aktuellen Bedrohungsszenarien eine noch geringere Relevanz zu, als die übrigen Branchen.

UMSETZUNG VON SCHUTZMASSNAHMEN IN UNTERNEHMENSBEREICHEN

- In den Unternehmen besteht ein Umsetzungsgefälle zwischen strategischen und operativ tätigen Arbeitsbereichen. Marketingabteilungen weisen in der Regel größere Defizite bei der Umsetzung von Sicherheitsmaßnahmen auf, als etwa der IT-Bereich selbst.

MASSIVE DEFIZITE IN ALLEN RELEVANTEN HANDLUNGSBEREICHEN

Technische Maßnahmen und Lösungen

- Die Umsetzung einfacher technischen Lösungen, wie Anti-Viren und Anti-Malware Tools weist bereits deutliche Defizite auf. Rund 60 % der befragten Unternehmen muss somit ein ungenügender Basisschutz attestiert werden.
- Anspruchsvollere technische Lösungen, wie Maßnahmen und Lösungen zur Datenverschlüsselung oder sicheren Kollaboration, werden vom Großteil der mittelständischen Unternehmen garnicht, oder unzureichend umgesetzt. Mehr als die Hälfte der befragten Unternehmen haben massiven Nachholbedarf bei der Umsetzung von Verschlüsselungslösungen.
- Sehr anspruchsvolle Lösungen, wie Unified Threat Mnagament, Intrusion Detection oder Data-Loss-Prevention sind bei der Mehrzahl der Unternehmen garnicht oder unzureichend umgesetzt.

Organisatorische Maßnahmen und Lösungen

- Organisatorische Maßnahmen, wie die Klassifizierung von Daten und Prozessen, die Schulung von Mitarbeitern sowie der Einsatz von Richtlinien und die Simulation von Ernstfallszenarien findet im überwiegenden Teil der befragten Unternehmen keine erfolgreichen Einsatz.

Rechtliche Maßnahmen und Lösungen

- Die rechtliche Absicherung, in Form der Definition von Zuständigkeiten und der Haftungsfragen im Ernstfall, aber auch der Einsatz von Geheimhaltungsvereinbarungen weist in mindestens der Hälfte der Unternehmen massive Defizite auf.

Strategische Maßnahmen und Lösungen

- Strategische Maßnahmen, wie die Festlegung einer unternehmensweiten IT-Security-Strategie oder die Abstimmung von Personal- und Budgetplanung auf den IT-Security-Bereich wird bei rund 60 % der befragten Unternehmen nicht hinreichend umgesetzt.

iii. Management Summary - Handlungsempfehlungen

- **Ein umfassendes Sicherheitskonzept ist unverzichtbar**
  Die Sicherheitsbemühungen nur auf eines der vier Handlungsfelder zu konzentrieren ist nicht zielführend. Technische Maßnahmen und Lösungen erfolgreich zu implementieren, bedeutet noch lang nicht, dass ein hinreichendes Schutzniveau erreicht wurde. Rechtliche, organiatorische und strategische Maßnahmen gehören ebenso zu einem umfassenden Sicherungskonzept. Während die technischen Maßnahmen und Lösungen in der Hauptsache zur Abwehr von Bedrohungen und Angriffen dienen, bilden die Maßnahmen und Lösungen des rechtlichen, organisatorischen und strategischen Handlungsfeldes überwiegend eine Absicherung des Unternehmens im Falle eines erfolgreichen Angriffs, um das Ausmaß negativer Konsequenzen zu begrenzen. Auch technisch bestens aufgestellte Unternehmen können zum Opfer eines gezielten Angriffs werden, der im Extremfall selbst die Geschäftsgrundlage bedroht. Ohne entsprechende Konzepte im Bereich von Backups, der Versicherung gegen Datenverlust und der Definition von Verantwortlichkeiten sind die Folgen erfolgreicher Angriffe unkalkulierbar.

- **Mitarbeiter sensibilisieren**

  Mitarbeiter sind nicht nur eine mögliche Gefahrenquelle, sie sind vielmehr ein wichtiger Baustein eines umfassenden Konzepts zur IT- und Informationssicherheit. Angesichts der aktuell Umsetzung technischer Maßnahmen und Lösungen.

  Wenn den Mitarbeitern bewusst ist, dass Ihr Handeln Auswirkungen auf die Sicherheit der Unternehmensdaten hat, lassen sich gemeinsam Regelwerke erarbeiten, die sowohl den Anforderungen der IT-Sicherheit genügen, wie auch den reibungslosen Ablauf des Tagesgeschäfts sichern.

- **Praktische Übungen zur IT-Sicherheit schaffen Awareness und zeigen Schwachstellen auf**
  Auch die besten technischen Lösungen können nur dann effizient sein, wenn ihr Einsatz auch beherrscht wird. Es genügt nicht entsprechnede technische Lösungen für den Ernstfall vorzuhalten, wenn keine Kapazitäten bestehen, diese auch einzusetzen. Übungen und Ernstfallsimulationen sind das Mittel der Wahl um zu überprüfen, ob Notfallpläne und Prozeduren auch in der Praxis funktionieren.
- **IT- und Informationssicherheit ist ein Prozess**
  Es ist ein Fehler anzunehmen, dass ein Unternehmen durch einmalige Planung und Investition auf lange Zeit in der Lage ist die Sicherheit von Daten und Informationen zu gewährleisten. Bedrohungsszenarien ändern sich, Angreifer werden durch guten Schutz in einem Bereich ermutigt alternative Angriffsflächen zu suchen, die Unternehmens-IT sieht sich somit täglich mit neuen Herausforderungen konfrontiert. Entsprechend müssen Sicherheitskonzepte kontinuierlich überprüft und weiterentwickelt werden. Besonders für Mittelständler

kann dies zum Problem werden, da eine solche kontinuierliche Weiterentwicklung einen enormen Ressourcenaufwand nach sich zieht. Externe Deinstleister können hier ein echter Mehrwert sein.

A Bedrohungsszenarien

A.1. WAHRGENOMMENE (SUBJEKTIVE) RELEVANZ DER BEDROHUNGSSZENARIEN

Die befragten Unternehmen wurden gebeten, verschiedene praxisrelevante Bedrohungsszenarien hinsichtlich deren Relevanz für das eigene Unternehmen zu bewerten. Abbildung 1 zeigt die branchenübergreifende Bewertung.

38% der Unternehmen sehen sich durch Viren und Würmer ernsthaft bedroht.

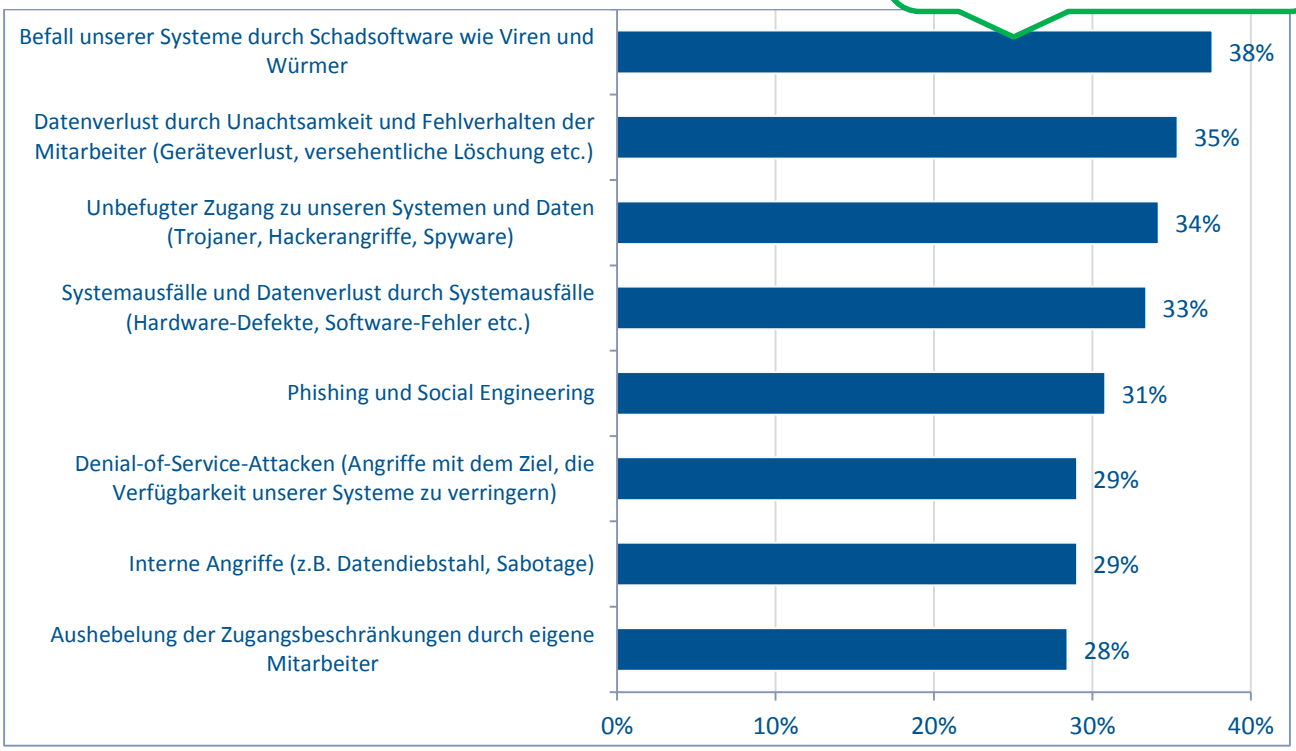

Abbildung 1: hohe und sehr hohe Relevanz ausgewählter Bedrohungen der IT- und Informationssicherheit (Anteil der Unternehmen mit mangelnder Umsetzung)

Mangelndes Problembewusstsein, trotz zahlreicher Negativbeispiele

Insgesamt ist das Problembewusstsein für die Relevanz der genannten Bedrohungsszenarien bei weitem nicht so stark ausgeprägt wie es nach den Entwicklungen und Negativbeispielen der letzten Jahre angemessen wäre. Über die Gründe für solch eklatante Fehleinschätzungen der Bedrohungslage kann keine generalisierte Aussage getroffen werden. Hauptverantwortlich dürften aber zwei zentrale Problemstellungen sein: Erstens die Annahme, das eigene Unternehmen werde schon nicht in den Fokus von Cyber-Kriminellen geraten. Zweitens eine grundlegend falsche Einschätzung der möglichen Konsequenzen erfolgreicher Cyber-Angriffe.

Konsequenzen von Bedrohungsszenarien werden falsch bewertet

Schadsoftware wie Viren und Würmer zählen zu den am weitesten verbreiteten Gefahrenquellen. Dabei ist das Gefährdungspotential des Großteils dieser Schädlinge überschaubar: Sie werden eher selten für spezifische Angriffe genutzt, sondern stellen eher eine allgegenwärtige „Grundgefährdung“ dar. Die hohe Relevanz, die Unternehmen der Bedrohung durch Viren und Würmer zuschreiben ist also einerseits durchaus berechtigt, die zu befürchtenden Konsequenzen sind aber in aller Regel überschaubar. Zumal der Schutz gegen diese Art der Bedrohung bereits weit verbreitet ist.

Geschäftsaufgabe in Folge gezielter Angriffe

Dass gezielten Angriffen eine deutlich geringere Relevanz beigemessen wird ist bedenklich und stellt ein weiteres Indiz für die Annahme dar, dass die Konsequenzen solcher Angriffe drastisch unterschätzt wird. Gezielten Attacken können für ein Unternehmen sehr schnell zu einem ernsten Problem werden, wobei ernst durchaus bedeuten kann, dass eine Geschäftsaufgabe am Ende einer erfolgreichen Attacke steht. So geschehen beim Hosting Dienstleister Code-Spaces. Nach einer massiven Attacke, bei der es sich vordergründig „lediglich“ um einen gezielten DDoS-Angriff zu handeln schien, kam es zeitgleich im Hintergrund zur Löschung von Benutzerdaten und Backups. Code-Spaces sah durch diesen Angriff seine Geschäftsgrundlage derart kompromittiert, dass der Geschäftsbetrieb im Folgenden eingestellt wurde. Besonders für Dienstleistungsunternehmen, deren Geschäftserfolg nicht selten mit Ihrem guten Ruf untrennbar verbunden ist, stellen derartige Attacken vor

Ein weiteres, in seiner Konsequenz bislang vergleichsweise weniger gravierendes Beispiel stellt der Diebstahl von Millionen Kundendaten inklusive zugehöriger Passwörtern bei der Handelsplattform Ebay dar. Anhand dieses Vorfalls wird deutlich, dass auch deutlich größere Unternehmen zum Opfer von Cyber-Angriffen werden können, auch wenn deren Schutzniveau deutlich höher einzuschätzen ist, als im Mittelstand üblich. Zwar hält sich der entstandene Schaden für Ebay-Kunden in Grenzen, es darf aber davon ausgegangen werden, dass die Attacke in der Bilanz von Ebay selbst Niederschlag finden wird. Relevant ist diese Atacke vor allem vor dem Hintergrund, dass Ebay über eine sehr gute technische Absicherung verfügt, aber dennoch zum Ziel und zum Opfer eines Angriffs werden konnte. Die Täter drangen mit

gestohlenen Anmeldedaten von Ebay-Mitarbeitern in die Systeme ein und konnten so die ausgefeilten Sicherheitskakaden umgehen. Offensichtlich wird damit, dass eine gute technische Absicherung allein noch lang keinen umfassenden Schutz beitet.

A.2. RELEVANZ DER BEDROHUNGSSZENARIEN IN BRANCHEN

Die befragten Branchen zeigen sich nicht homogen bei der Bewertung der Relevanz einzelner Bedrohungsszenarien. In Abbildung 2 wird das Ausmaß der Unterscheide zwischen den Branchen deutlich.

46% der Industrie-Unternehmen halten ihre Daten durch die eigenen Mitarbeiter für gefährdet.

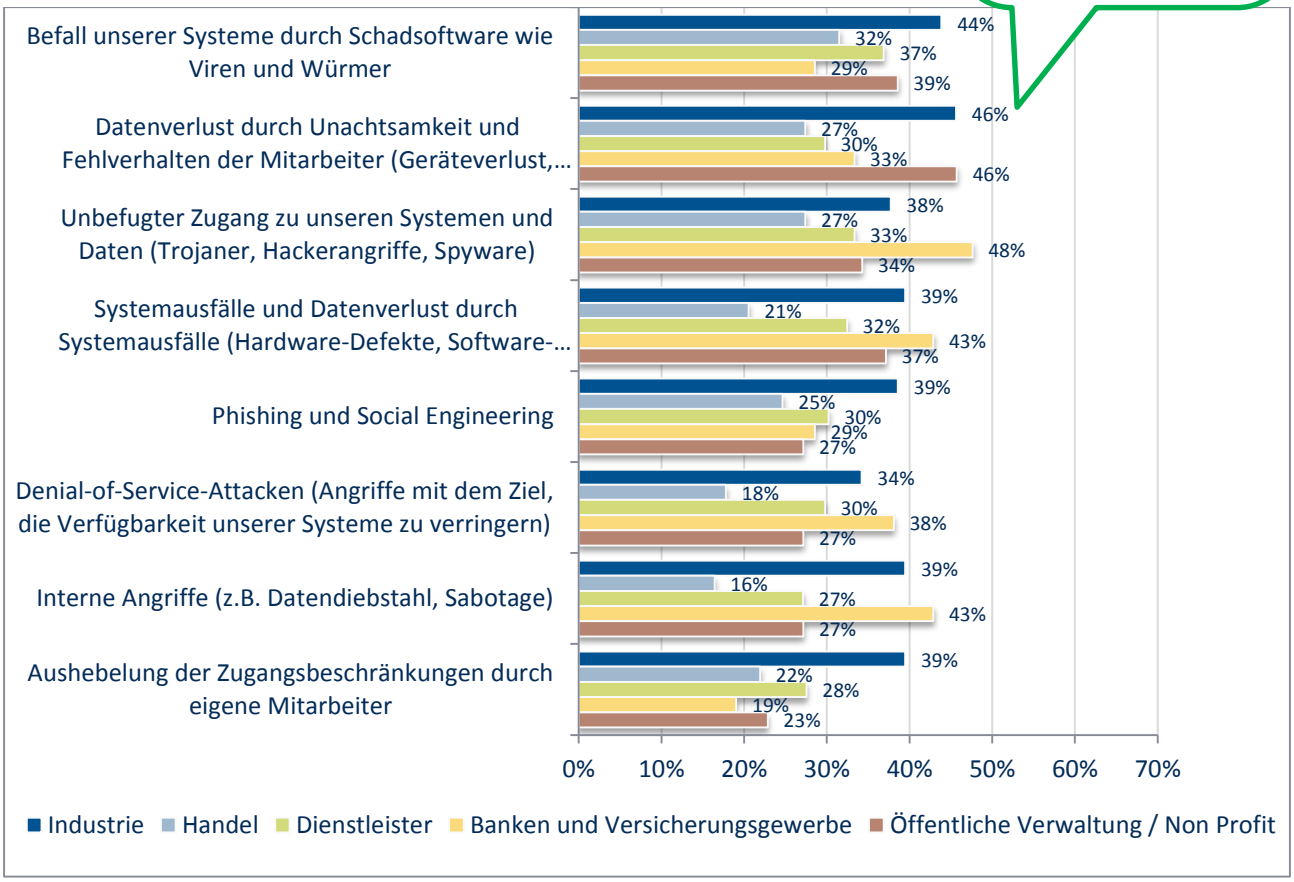

Abbildung 2: hohe und sehr hohe Relevanz ausgewählter Bedrohungen der IT- und Informationssicherheit (Anteil der Unternehmen mit mangelnder Umsetzung, Übersicht nach Branchen)

In der Industrie, wie auch bei Banken und Versicherungen ist der Sensibilisierungsgrad noch am höchsten: In beiden Branchen liegt der Anteil der Unternehmen, die eine hohe Relevanz der einzelnen Szenarien für die unternehmensweite IT- und Informationssicherheit wahrnehmen, deutlich über dem Durchschnitt der übrigen Branchen.

Banken und Versicherungen – Sensibilisiert aus Tradition

Bei Banken und Versicherungen stellt sich die Situation sehr eindeutig dar. Die Sensibilität Ihres Geschäftsfeld ist ihnen deutlich bewusst und ebenso wie die Tatsache, dass ihr Kerngeschäft sie beinahe traditionell in den Fokus Krimineller rückt. Die Verlagerung ihres Geschäftsbetriebes hin zur elektronischen Datenverarbeitung hat daran nicht geändert. Im Gegenteil, die Planung *umfassender* Sicherheitsstrategien gehört zum Kern ihrer Geschäftstätigkeit. So ist es nicht verwunderlich, dass es gerade die Banken sind, die Cyber-Bedrohungen am realistischsten, d.h. als reale Bedrohung ihres Kerngeschäfts ansehen. Zudem verfügen die Banken über langjährige Erfahrungen in der Sicherung externer Datenkommunikation. Online-Banking ist eine dieser Erfahrungsquellen, ebenso wie der Hochgeschwindigkeitshandel an internationalen Handelsplätzen.

Industriespionage – Mittelständler vs. professionelle Cyberangriffe

Der erhöhte Sensibilisierungsgrad von Industrieunternehmen resultiert aus der eigenen Einschätzung der Konsequenzen eines Verlusts von Daten aus Forschung/Entwicklung, Produktionsunterlagen, ebenso wie Dokumenten über Lieferantenbeziehungen. Dass selbst ausländische Geheimdienste in solche Formen der Industriespionage involviert sind, zeigt zum einen, welche Relevanz die Unternehmensdaten für Wettbewerber haben, zum anderen auch, mit welch professionellen Mitteln dieser Kampf geführt wird. Eine besondere Bedeutung ergibt sich dabei auf Grund aktueller Entwicklungen, die unter dem Schlagwort Industrie 4.0 zusammengefasst werden. Große Datenmengen, die zentral zur Verfügung gestellt werden, bieten Unternehmen enorme Möglichkeiten die eigenen Prozesse zu optimieren, sie eröffnene aber gleichzeitig neue Handlungsfelder für Cyber-Attacken. Hier entstehen in den Unternehmen, neben den bereits bekannten, neue Angriffspunkten, die in einer umfassenden Security-Strategie berücksichtigt werden müssen.

Industrie 4.0 schafft neue Angriffsfelder

Embedded Systems geraten in den Fokus

Neben der Absicherung des Unternehmens selbst gewinnt allerdings auch die Absicherung der Produkte zunehmend an Bedeutung. Besonders plakativ zeigt sich dies in der Fahrzeugindustrie und bei den Produkten ihrer Zulieferer. Mit steigendem Einsatz eingebetteter Systeme (embedded Systems) und deren zunehmenden Vernetzung steigt auch der Grad der Anfälligkeit für ge-

zielte Attacken. So gelang es Studenten in diesem Jahr die Sicherheitsbarrieren eines Tesla-Elektroautos zu überwinden und teile der Fahrzeugelektronik zu übernehmen, allerdings im Rahmen eines Wettbewerbes und ohne böse Absicht. Es wird aber deutlich ersichtlich, dass IT-Sicherheit in immer mehr Bereichen eine Rolle spielt und entsprechende Schutzmaßnahmen auch hier zu berücksichtigen sind.

Öffentliche Verwaltungen sehen sich nicht als potentielle Opfer

Weitaus geringer werden die Bedrohungen bei öffentlichen Verwaltungen und Non-Profit Unternehmen wahrgenommen. Sie machen das Hauptrisiko bei ihren eigenen Mitarbeitern aus und befürchten am ehesten den Datenverlust durch deren Unachtsamkeit oder Fehlverhalten. Externe, gezielte Attacken, etwa eine Kompromittierung ihrer Systeme durch Phishing-Attacken oder gezielte Hacks ihrer Systeme befürchten sie deutlich seltener als die übrigen Branchen.

MDM – Branchenübergreifendes

Kein neuer Trend, aber durch stärkere Verbreitung über Branchengrenzen hinweg zunehmend bedeutsamer, stellt sich der Einsatz mobiler Endgeräte im Unternehmen dar. Egal ob es sich dabei um dienstlich gelieferte Hardware handelt, oder ob private Geräte für dienstliche Zwecke (BYOD) genutzt werden, die Herausforderungen für die Unternehmens-IT wächst. Der wachsende Markt der Mobile Device Management (MDM) Lösungen belegt, dass die Relevanz einheitlichen Managements mobiler Endgeräte einen überaus wichtigen Baustein Beitrag zur umfassenden Security-Strategie darstellt.

A.3. WAHRGENOMMENE UMSETZUNGSDEFIZITE VON SCHUTZMAßNAHMEN GEGEN DEFINIERTE BEDROHUNGSSZENARIEN

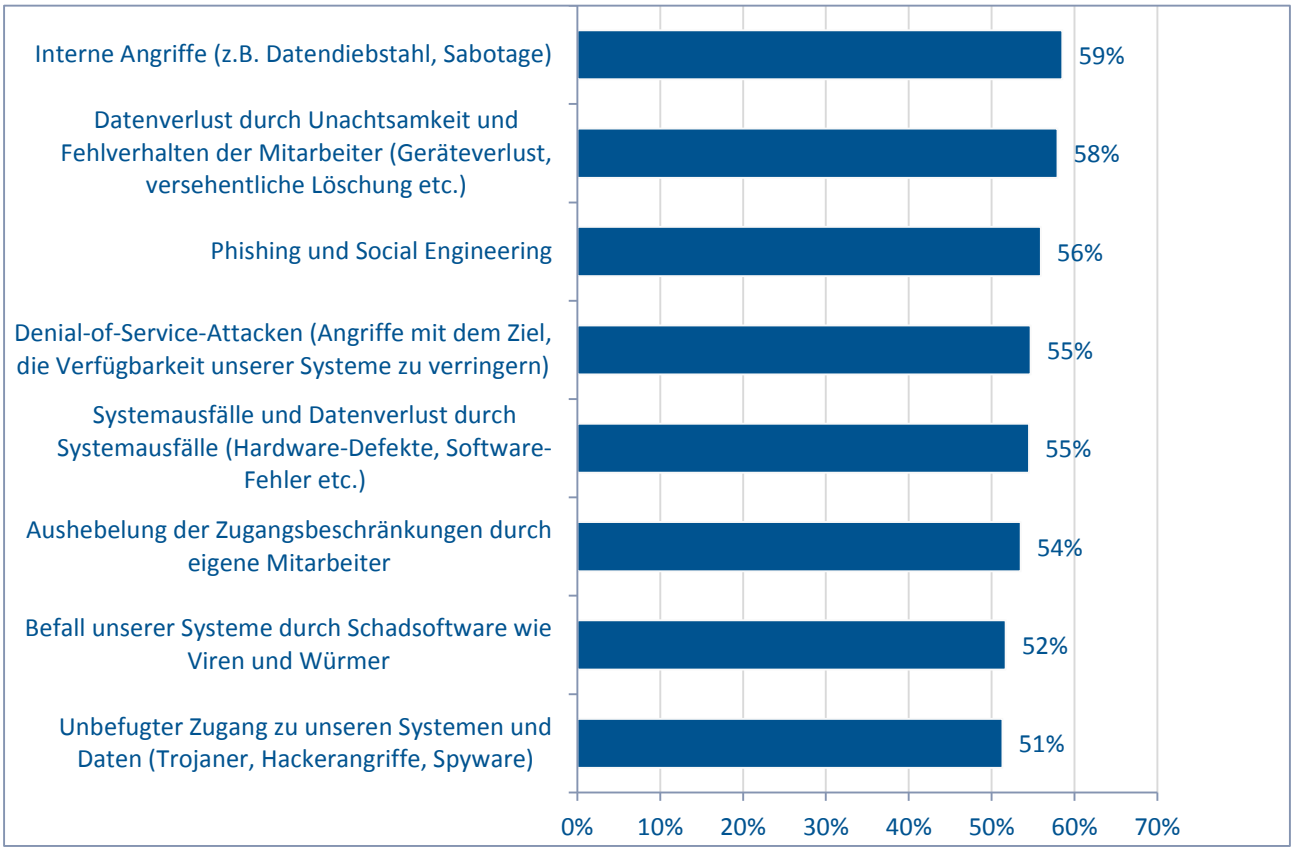

Abbildung 3: Defizite beim Schutzes gegen Bedrohungen der IT- und Informationssicherheit (Anteil der Unternehmen mit mangelnder Umsetzung)

59% aller Unternehmen bewerten den Schutz vor internen Angriffen als unzureichend.

Das einzig positive Fazit, das an dieser Stelle gezogen werden kann, ist, dass einem großen Teil der Unternehmen durchaus bewusst ist, dass ihre bisherigen Schutzmaßnahmen unzureichend sind. Mehr als jedes zweite Unternehmen ist sich bewusst, dass die vorhandenen Daten und Informationen nicht hinreichend gesichert sind und dass sie jederzeit Opfer eines gezielten Angriffs werden können.

Zahl der Attacken steigt - dringender Nachholbedarf im deutschen Mittelstand

Schon anhand dieser subjektiven Sichtweise wird klar, wie schlecht es im deutschen Mittelstand um IT- und Informationssicherheit bestellt ist, dringender Nachholbedarf besteht bei über der Hälfte der Unternehmen. Noch ist die Zahl der Angriffe überschaubar, aber im Trend ist eine deutliche Zunahme erkennbar. Unternehmen müssen sich hier schnellstmöglich besser aufstellen und sollten sich nicht darauf verlassen, dass sie schon nicht ins Visier von Cyber-Kriminellen geraten.

B Umsetzung von IT- und Informationssicherheit in einzelnen Geschäftsbereichen

B.1. ANALYSE DER GESCHÄFTSBEREICHE (BRANCHENÜBERGREIFEND)

Nachdem in Kapitel 1 ersichtlich wurde, welche Relevanz einzelnen Bedrohungsszenarien von den Unternehmen zugeschrieben wird und wie die einzelnen Branchen sich dabei unterscheiden, gilt der Fokus im Folgenden den verschiedenen Geschäftsbereichen innerhalb der Unternehmen. Abbildung 3 zeigt die Defizite in der Umsetzung von Schutzmaßnahmen getrennt für die einzelnen Funktionsbereiche.

In 58% der Unternehmen existieren IT-Security Defizite in den Marketing Abteilungen

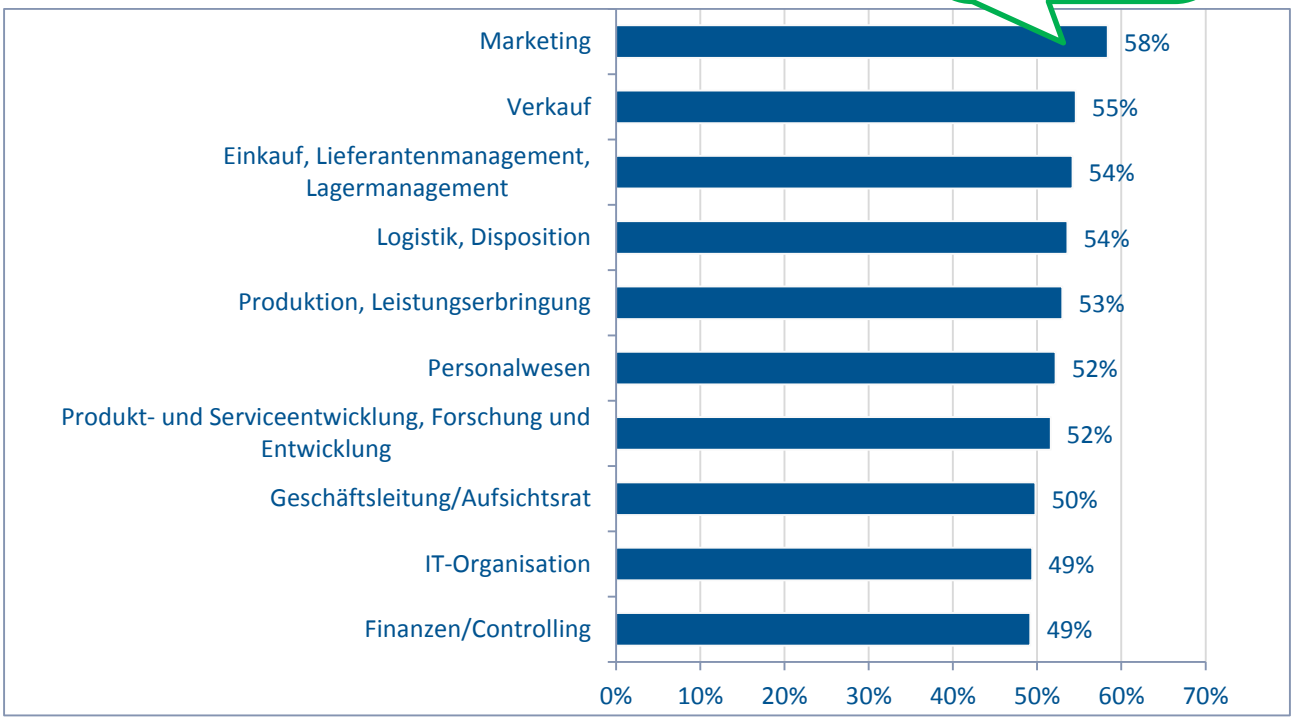

Abbildung 4: Defizite der Umsetzung von IT-Sicherheit in den Unternehmensbereichen (Anteil der Unternehmen mit mangelnder Umsetzung)

Konsequenzen von Bedrohungsszenarien werden falsch bewertet

Die deutlichsten Defizite werden, branchenübergreifend, in den operativ tätigen Unterenhmensbereichen berichtet. Rund 60 Prozent der befragten Unternehmen machen in den Marketingabteilungen die größten Defizite aus. Mit nur geringem Abstand folgen weitere operativ tätige Abteilungen. Selbst im Personalwesen, das strikten gesetzlichen Regularien unterliegt, stellt sich die Situation kaum positiver dar.

Nur in geringem Maße besser wird die Umsetzung von Schutzmaßnahmen in den strategisch tätigen Geschäftsbereichen der

Geschäftsleitung, IT-Organisation und Finanzen/Controlling beurteilt. Insbesondere im Bereich der IT-Organisation sind diese Defizite überraschend, gehört doch die Umsetzung des größten Teils möglicher Maßnahmen und Lösungen zur IT- und Informationssicherheit zu den Kernaufgaben der IT-Abteilungen.

Abteilungsübergreifende Defizite in der IT- und Informationssicherheit

Ebenso bedenklich sind die Sicherheitsdefizite in den Bereichen Geschäftsleitung und Finanzen/Controlling zu bewerten. Vor allem unter dem Aspekt der Sensibilität der dort verarbeiteten Daten und unter Berücksichtigung der möglichen Konsequenzen von Sicherheitslecks ist ein solch geringes Schutzniveau bei nahezu 50 Prozent der Unternehmen ein alamierendes Ergebnis.

Besonders kritisch aber sind die genannten Defizite an IT- und Informationssicherheit im Bereich des Personalwesens. Neben möglichen Auswirkungen auf die operative und stategische Tätigkeit der Unternehmen drohen hier auch juristische Konsequenzen für die Unternehmen.

Kontaktinformationen

ÜBER TECHCONSULT

Die techconsult GmbH, gegründet 1992, zählt zu den führenden Analystenhäusern in Zentraleuropa. Der Schwerpunkt der Strategieberatung liegt in der Informations- und Kommunikationsindustrie (ITK). Durch jahrelange Standard- und Individual-Untersuchungen verfügt techconsult über einen im deutschsprachigen Raum einzigartigen Informationsbestand, sowohl hinsichtlich der Kontinuität als auch der Informationstiefe, und ist somit ein wichtiger Beratungspartner der CXOs sowie der IT-Industrie, wenn es um Produktinnovation, Marketingstrategie und Absatzentwicklung geht.

Die techconsult GmbH wird von den geschäftsführenden Gesellschaftern und Gründern Peter Burghardt und Andreas W. Klein am Standort Kassel mit einer Niederlassung in München geleitet und ist Teil der Heise Medien Gruppe.

techconsult GmbH

– The IT Market Analysts –

Baunsbergstr. 37

34131 Kassel

Tel. +49 561 – 8109 -0

Fax +49 561 – 8109 -101

http://www.techconsult.de

Sponsoren

Fortinet betreut mit ca. 2.300 Mitarbeitern und ca. 9.000 Vertriebspartnern weltweit über 100.000 Kunden aller Branchen und Größenordnungen. Fortinet ist seit vielen Jahren die Nr. 1 im UTM-Security-Markt. Fortinets Next-Generation-Security-Lösungen beinhalten ein breites Spektrum an Sicherheits-Modulen und sind daher bestens geeignet für die Absicherung von Unternehmensnetzen oder Produktionssystemen. Speziell entwickelte Chipsets beschleunigen gezielt einzelne Prozesse und garantieren so Security in Echtzeit.

Die baramundi software AG bietet Management-Software für Clients, Server und mobile Geräte. Der Fokus liegt dabei auf sicherem Management von Arbeitsplatzumgebungen, plattformübergreifend und für verschiedenste Endgeräte, sowie auf Compliance- und Schwachstellenmanagement.

IBM Security bietet beim Thema Unternehmenssicherheit eines der innovativsten Produkt- und Serviceportfolios mit dem höchsten Integrationsfaktor. Das Lösungsportfolio, das von der weltweit anerkannten X-Force-Forschungs- und Entwicklungsgruppe unterstützt wird, stellt Sicherheitsdaten bereit, mit denen Unternehmen mit einem ganzheitlichen Ansatz Mitarbeiter, Infrastrukturen, Daten und Anwendungen schützen können. Hierfür steht eine große Anzahl von Lösungen für die unterschiedlichsten Bereiche zur Verfügung: Identitäts- und Zugriffsmanagement, Datenbanksicherheit, Anwendungsentwicklung, Risikomanagement, Endpunktmanagement, Netzwerksicherheit und vieles mehr. Mit diesen Lösungen können Unternehmen ihr Risikomanagement wesentlich effektiver gestalten und integrierte Sicherheitsmechanismen für Mobile-, Cloud-, Social Media- und andere Geschäftsarchitekturen implementieren. IBM betreibt eine der weltweit größten Organisationen im Bereich der Erforschung, Entwicklung und Bereitstellung von Sicherheitslösungen, verwaltet die Überwachung von 13 Mrd. Sicherheitsereignissen pro Tag in mehr als 130 Ländern und besitzt über 3.000 Sicherheitspatente.

Die MESH GmbH bietet maßgeschneiderte Datacenter-, Cloud- und Connectivity-Services für den Mittelstand und unterstützt Unternehmen beim Outsourcing der Infrastruktur in sichere IT-Rechenzentren. Bei den MESH Trusted Cloud Lösungen können zusätzlich Private-, Community- oder Hybrid-Cloud Services individuell betrieben und miteinander kombiniert werden. ISO-zertifizierte Rechenzentren sowie sichere Netzwerkdienste durch Multi-Tier I Carrier-Anbindungen garantieren eine hohe Verfügbarkeit und Ausfallsicherheit.

Die Microsoft Deutschland GmbH richtet sich mit seinem Safety & Security Center mit Sicherheitshinweisen und Hintergrundartikeln an alle IT-Anwender, die ihre IT-Umgebungen schützen wollen. Das Safety & Security Center bietet neben allgemeinen Informationen auch praktische Hinweise, z. B. wie Angriffsversuche zu erkennen und abzuwenden sind.

Die NCP engineering GmbH ist technologischer Weltmarktführer für Lösungen rund um den ferngesteuerten Zugriff auf zentrale Datenbestände und Ressourcen von Unternehmen. NCP liefert Produkte, Spitzentechnologie, zentrales Remote Access Management und End-to-Site Sicherheit „aus einer Hand“.

Die Sophos GmbH hat sich der Sicherheit und dem Schutz aller existierenden Endpoints von Netzwerken verschrieben. Durch individuelle, an Unternehmensanforderungen angepasste Produkte können alle Geräte eines Netzwerks zuverlässig, einfach und zentral in der Cloud verwaltet werden.

Telekom bietet Anwendern komplette IT Sicherheit: beginnend mit Checks und Consulting (IT Security Checks) über umfassende Sicherheit für Unternehmensnetze (Managed Network Security) und volle Sicherheit für feste und mobile IT Arbeitsplätze (Managed Endpoint Security) bis hin zur Sicherheit für sensible Kommunikation und Daten kombiniert (Managed Communication Security).

Network Box liefert umfassende und gemanagte IT-Sicherheitslösungen für Unternehmensnetzwerke. Seit mehr als 14 Jahren weltweit auf dem Markt aktiv, sorgt Network Box als Entwickler, Hersteller und Managed Security Service Provider(MSSP) mit skalierbaren und modularen Systemen für ein Höchstmaß an Sicherheit in Unternehmen. Zu den gemanagten Sicherheits-Appliances gehören: Firewall, VPN, IDP, Anti-Malware, Content-Filtering, WAF, Anti-DDos, live Monitoring, Reporting, uvm. Alle Sicherheits-Features werden über die patentierte PUSH-Technologie in Sekunden schnelle auf dem neusten Stand gehalten.