IDC MULTI-CLIENT-PROJEKT

IT-SECURITY IN DEUTSCHLAND 2018

Herausforderungen und Pläne

IDC ANALYZE THE FUTURE

JULI 2018

GESPONSERT VON MATRIX42

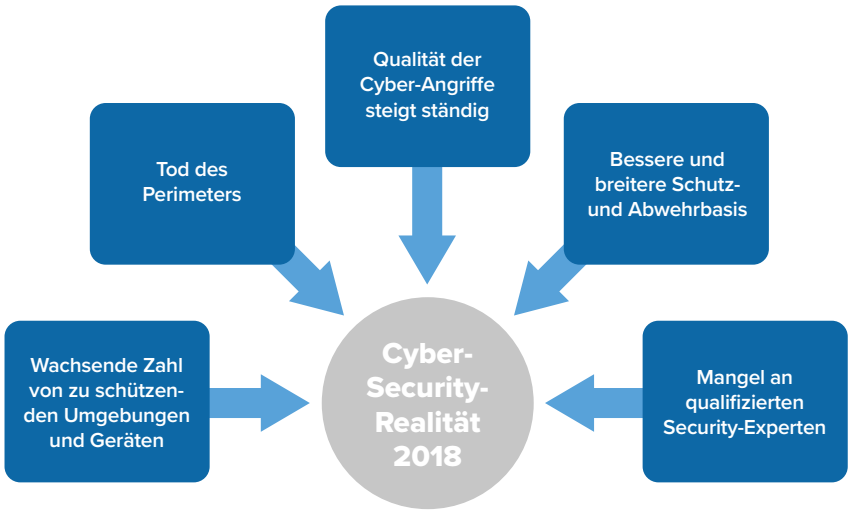
IT-SICHERHEIT MUSS VIELFÄLTIGE HERAUSFORDERUNGEN BEHERRSCHEN

IT-Sicherheit ist und bleibt ein Dauerbrenner in den IT-Abteilungen und für jeden Mitarbeiter in den Fachbereichen. Dafür lassen sich folgende Ursachen benennen:

- Ein zentraler Faktor ist die digitale Transformation. Mit ihr sind alle Firmen aufgefordert, ihre IT-Security zu überprüfen und neu auszurichten. Die umfassende Prozessautomatisierung und das Agieren in Ökosystemen mit Partnern, Lieferanten und Kunden – wichtige Aspekte der Digitalisierung von Geschäftsprozessen – gehen mit einer umfassenden Vernetzung von IT und IP-basierten Geräten Hand in Hand. Die Folge: Cloud Computing, das Internet der Dinge (IoT), Virtualisierung, offene Schnittstellen (APIs) und IT-Systeme sind Angriffspunkte, die intelligent abgesichert werden müssen.
- Gesetzliche Vorgaben, Regelwerke und Compliance-Anforderungen und der damit verbundene Datenschutz – Stichwort: EU-DSGVO – sowie die Absicherung der IT-Systeme, die in kritischen Infrastrukturen (Kritis) betrieben werden, zwingen ebenfalls zu neuen Investitionen in die IT-Sicherheit.
- Zudem müssen alle Unternehmen und Organisationen zwei grundsätzliche Arten von Angriffen parieren. Da sind zunächst die alltäglichen und täglich laufenden Attacken, mit denen die Hacker das Web nach dem Gießkannen-Prinzip fluten. Diese Attacken zielen auf die Mitarbeiter in den Fachabteilungen und auf unsere privaten Accounts. Als Faustregel kann gelten, dass 5 bis 10 Prozent der User auf Links in Phishing-Mails klicken. Auf der anderen Seite stehen ausgefeilte Cyber-Attacken. Diese zielen typischerweise auf eine Person oder eine spezifische Information. Das Ziel rechtfertigt einen hohen Aufwand: diese Angriffe laufen mehrstufig, über einen längeren Zeitraum und nutzen unterschiedliche Methoden.

Die Häufigkeit und die Qualität von Cyber-Attacken wird in den nächsten Monaten weiter steigen. Es geht fast immer um Geld: Erpressung, wirtschaftlichen Vorteil, Rufschädigung usw.

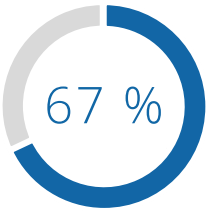
Abbildung 1: Fünf grundlegende Security-Trends



Quelle: IDC Market Analysis Perspective, Worldwide Security Products, September 2017

SICHERHEIT PROAKTIV ANGEHEN, SECURITY-FOKUS NEU DEFINIEREN

Die Studie belegt, wie kritisch die Security-Lage in Unternehmen und Organisationen in Deutschland ist. 67 Prozent der befragten Unternehmen geben an, in den letzten Monaten Sicherheitsvorfälle verzeichnet zu haben. Am häufigsten waren PCs und Notebooks (34 Prozent), Netzwerke (31 Prozent) sowie Smartphones und Tablets (30 Prozent) betroffen. Das ist insofern kritisch, als sie als Einfallstor in das Rechenzentrum genutzt werden. Aber auch die Rechenzentren selbst (29 Prozent) und Server (28 Prozent) waren ebenso wie Drucker, Sensoren und IoT – wenn auch in geringerem Maße – betroffen. Jede IP-Adresse bietet eine Angriffsfläche, die minimiert werden muss, und ausnahmslos jeder Mitarbeiter ist ein potenzielles Angriffsziel. Das gilt für den Pförtner genauso wie für den Vorstandsvorsitzenden. Es ist also höchste Zeit, IT-Sicherheit in Ihrem Unternehmen proaktiv, strategisch und gesamtheitlich anzugehen.



der Unternehmen waren in den vergangenen 24 Monaten von Sicherheitsvorfällen betroffen

Viele Organisationen haben es bislang nicht geschafft, das Sicherheitsrisiko durch Anwender in den Griff zu bekommen. Das Fehlverhalten der Anwender oder mangelnde Awareness, wie etwa durch die Reaktion auf Phishing-Mails, Downloads unsicherer Apps oder Geräteverluste, hat auch in den letzten Monaten wieder Tür und Tor zu Firmendaten für Externe geöffnet. Somit überrascht es nicht, dass das Fehlverhalten der Anwender (37 Prozent) sowie unzureichend gesicherte Endpoints (34 Prozent) die beiden am häufigsten genannten Sicherheitsrisiken sind, noch vor Aktivitäten von Cyber-Kriminellen.

Abbildung 2: Die größten Sicherheitsrisiken in Unternehmen

1. Falsche Benutzung, mangelnde Awareness der Anwender
2. Ungesicherte oder mangelhaft gesicherte Endpoints
3. Malware, Phishing und Social Engineering oder DoS-Angriffe
4. Vorsätzliches Anwenderfehlverhalten
5. Vernetzung von Geräten und Anwendungen

N = 230 Unternehmen

IDC hat im Juni 2018 eine primäre Marktbefragung durchgeführt, um Einblicke in die Umsetzungspläne, Herausforderungen und Erfolgsfaktoren von deutschen Unternehmen bei der Absicherung der IT und der Geschäftsprozesse zu erhalten. Anhand eines strukturierten Fragebogens wurden branchenübergreifend 230 Organisationen in Deutschland mit mehr als 20 Mitarbeitern befragt. Der vorliegende Executive Brief bietet IT- und Fachbereichsentscheidern auf Basis der Studien-Highlights Best Practices und Empfehlungen für die Stärkung der IT-Sicherheit in ihrem Unternehmen.

FÜNF RATSCHLÄGE FÜR EINE HÖHERE IT-SICHERHEIT

Die folgenden fünf Empfehlungen sollen Ihnen Anregungen und Impulse vermitteln, um den Schutz der IT zu verbessern und damit die Aufrechterhaltung betrieblicher Abläufe zu stärken.

Ratschlag 1: Führen Sie eine realistische Bestandsaufnahme der Schutz-, Abwehr- und Wiederherstellungsfähigkeit Ihres Unternehmens durch

In sehr vielen Unternehmen treffen wir immer wieder auf historisch gewachsene IT-Security-Landschaften. Sie umfassen nicht selten 50 bis 80 unterschiedliche Security-Lösungen, entweder als On-Premises-Software-Lösung, Appliance, Security-as-a-Service oder Managed Security Service. Eine transparente Übersicht über alle Lösungen, die in den meisten Fällen in den klassischen Security-Silos Endpoint-, Messaging-, Network- und Web-Security anzutreffen sind, fehlt häufig. Somit ist Transparenz ein erster wichtiger Schritt in Richtung stärkere IT-Security.

Gleichzeitig sollten Sie sich die Frage beantworten, ob und wie gut Ihr Cyber-Security-Risiko-Management, beispielsweise nach NIST, die fünf Punkte „Identify – Protect – Detect – Respond – Recover" abdeckt. Sie helfen Ihnen dabei, an die Bestandsaufnahme eine Neubewertung Ihrer IT-Security anzufügen. Die Studie zeigt, dass bislang weniger als die Hälfte der befragten Unternehmen den Schritt der Neubewertung vom bisher dominierenden „Prevent und Protect", d. h. einer eher reaktiv orientierten Sicherheitslandschaft, hin zu „Detect und Respond" mit dem Ziel einer kontinuierlichen Überwachung in Echtzeit und entsprechenden Maßnahmen als Reaktion auf Auffälligkeiten im System gegangen ist.

Beschränken Sie Ihre Bestandsaufnahme nicht nur auf die zentrale IT-Organisation. Beziehen Sie die Fachbereiche mit ein. Fachabteilungen und Geschäftsbereiche schaffen in der Regel in Eigenverantwortung Software und Hardware an oder nutzen Cloud Services. Dabei kommt es häufig zur Verletzung der Compliance. Entweder weil die entsprechenden Regeln nicht bekannt sind oder weil sie schlichtweg ignoriert werden. Auch wenn der Begriff Schatten-IT etwas in den Hintergrund gerückt ist, so besitzt er nach wie vor eine volle Gültigkeit zur Kategorisierung der IT-Ressourcen, die außerhalb der zentralen IT-Organisation verwaltet werden.

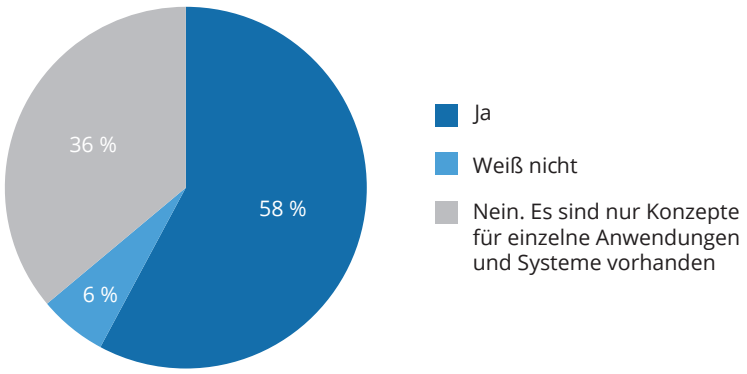
Zur Bestandsaufnahme müssen unbedingt auch Drucker zählen, denn sie dienen Angreifern immer häufiger als Einfallstore in die Unternehmen. Zwar ist in den meisten Unternehmen ein Basisschutz der Endgeräte vorhanden, eine umfassende Betrachtung des Schutzes über den gesamten Lifecycle von PCs, Druckern und Multifunktionsgeräten fehlt aber häufig. Der Grund: Viele Unternehmen sehen hier nur ein geringes Risiko für den Verlust von Daten oder für Angriffe auf die Unternehmens-IT, oder sie haben das gesamte Print-Management in die Hände von Managed Print Service Providern gelegt.

Wie Sie sehen, umfasst eine Bestandsaufnahme eine Vielzahl von Bereichen und Aufgaben. Bleiben Sie aber nun nicht auf halbem Wege stehen. Der Bestandsaufnahme müssen immer Aktivitäten zur Verbesserung der IT-Sicherheit folgen.

Ratschlag 2: Betrachten Sie IT-Security ganzheitlich und planen Sie strategisch

IT-Security-Lösungen, -Technologien und -Services entfalten ihre Wirkung nur innerhalb umfassender Konzepte. Lediglich 58 Prozent der Unternehmen verfügen über ein zentrales Konzept für Informationssicherheit, das alle Systeme und Geräte umfasst. Das ist eine zu geringe Zahl. Wir raten grundsätzlich zu einem zentral ausgerichteten Ansatz. Andernfalls bleibt die Gefahr groß, Lücken und somit potenzielle Angriffspunkte nicht ausreichend abzusichern. Das ist ein essentieller Punkt, den Sie immer im Hinterkopf haben sollten.

Abbildung 3: Verfügt Ihr Unternehmen über ein zentrales Konzept zur Informationssicherheit?



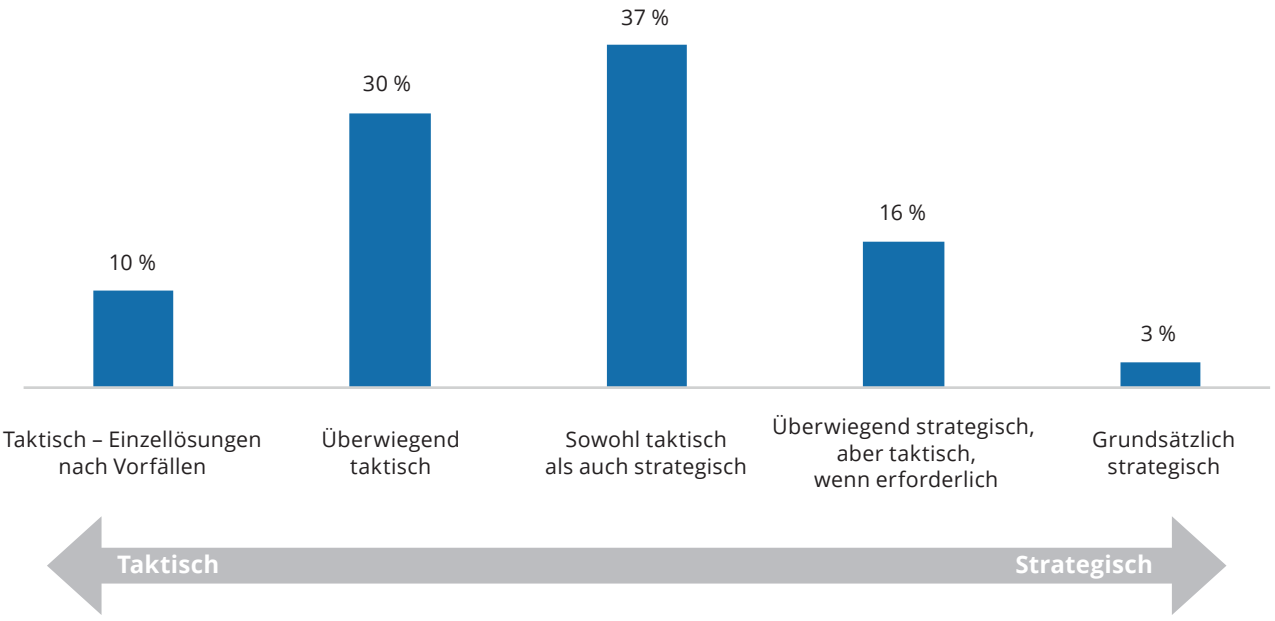
N = 230 Unternehmen

Orientieren Sie sich bei der Konzeption ganzheitlicher Konzepte an den gängigen Best-Practice- und Sicherheits-Frameworks von NIST, ENISA oder vom BSI. Immerhin 82 Prozent Ihrer Kollegen orientieren sich an IT-Security-Best-Practice und betrachten sie als ein probates Mittel zur Verbesserung der Security-Prozesse. Bemühen Sie sich, diese Frameworks in so vielen Security-Domains wie möglich umzusetzen. Das ist zugegebenermaßen keine einfache Aufgabe und häufig mit einem hohen Aufwand verbunden.

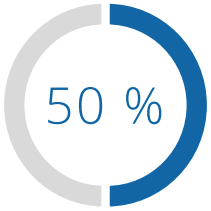
Viele IT-Security-Verantwortliche führen zu Beginn des Lifecycles neuer Lösungen oder Initiativen eine Risikoklassifizierung durch. Diese wird über den Lifecycle aber in vielen Fällen nicht geändert oder modifiziert. Wir empfehlen dringend einmal jährlich eine Risikobewertung und Klassifizierung Ihrer IT.

Zu den größten Herausforderungen in diesem Zusammenhang zählt die Bereitstellung von finanziellen Mitteln. Es fällt immer wieder auf, dass Unternehmen nach großflächigen Angriffswellen wie durch WannaCry oder Petya hektisch und aktionistisch reagieren und kurzfristig Budgets bereitstellen. Sie könnten solchen Attacken gelassener entgegensehen, wenn Sie sich bereits im Vorfeld gezielt mit Anschaffungen, beispielsweise von Back-up- und Recovery-Lösungen, auf solche Angriffe vorbereiten würden. Aus unserer Sicht ist die Bereitschaft, strategisch in Security zu investieren, noch nicht ausreichend umfassend entwickelt. Hier empfehlen wir Ihnen, gemeinsam mit der Geschäftsführung und den Fachbereichen an einer Lösung zu arbeiten.

Abbildung 4: Investieren Sie in Ihrem Unternehmen eher taktisch (Einzellösungen nach Erfordernis) oder strategisch (auf Basis einer definierten Planung) in IT-Security-Lösungen?



N = 230, Mehrfachnennungen



Weniger als 50 Prozent der Unternehmen haben ihre Security-Prozesse umfassend automatisiert

Ratschlag 3: Integrieren Sie Ihre Tools und automatisieren Sie Ihre Prozesse

IT-Security, die auf der Höhe der Zeit ist, besteht aus einem klaren, möglichst umfassenden Konzept, der Bereitschaft zu investieren, einem Lösungsmix aus etablierten und neuen Lösungen, der alle eingangs geschilderten Herausforderungen berücksichtigt, sowie aus der Automatisierung von Prozessen.

Basisschutzmechanismen wie Antimalware, Spamabwehr und Firewalls sind in praktisch allen Unternehmen vorhanden. Diese Mechanismen als Einzellösungen reichen aber längst nicht mehr aus. Die Mehrheit der befragten Unternehmen – konkret sind es zwei Drittel – betrachten die Integration als erforderlich für bessere Schutz- und Abwehrfähigkeiten und haben immerhin erkannt, dass ein integrativer Ansatz besser als die Summe aller Security-Lösungen schützt. Integrative Ansätze lassen sich auf unterschiedliche Art und Weise umsetzen. Hierzu zählen die Integration von Lösungen eines Anbieters oder unterschiedlicher Anbieter, die Orchestrierung verschiedener Lösungen, die Synchronisation auf Basis eines Kommunikations-Layers oder die Korrelation zwischen verschiedenen Lösungskomponenten. Lassen Sie sich von Ihren Anbietern aufzeigen, welche Formen der Integration sie heute bereits unterstützen und welche Schritte, beispielsweise auch in Richtung APIs und Konnektoren, sie in den nächsten ein bis zwei Jahren planen. Die Integration, Synchronisation, Orchestrierung oder Korrelation zwischen verschiedenen Lösungskomponenten ist nach Einschätzung von IDC ein absolut zwingender Schritt für End-to-End-Security-Architekturen.

Neben der Integration zählt auch die Automatisierung zu den wichtigsten Themen auf der Security-Agenda. Das ist ein Ansatz, der viel Potenzial für die Entlastung von Ressourcen bietet, sich in den Unternehmen jedoch noch nicht umfassend durchgesetzt hat. Zwar zeigt sich in der Befragung deutlich, dass 80 Prozent der Unternehmen damit begonnen haben, ihre IT-Security-Abläufe zu automatisieren, dies allerdings in vielen Fällen nur punktuell. In erster Linie zielt Automatisierung auf die Entlastung von Mitarbeitern. Manuelle Tätigkeiten wie das Patchen von Systemen, das Aufsetzen von Servern oder das Konfigurieren von Firewalls möchten viele IT-Security-Verantwortliche gern reduzieren, um mehr Zeit und Ressourcen für andere Tätigkeiten zu haben. Bei manuellen Tätigkeiten ist zudem die Gefahr der Fehlkonfiguration der Lösungen sehr hoch.

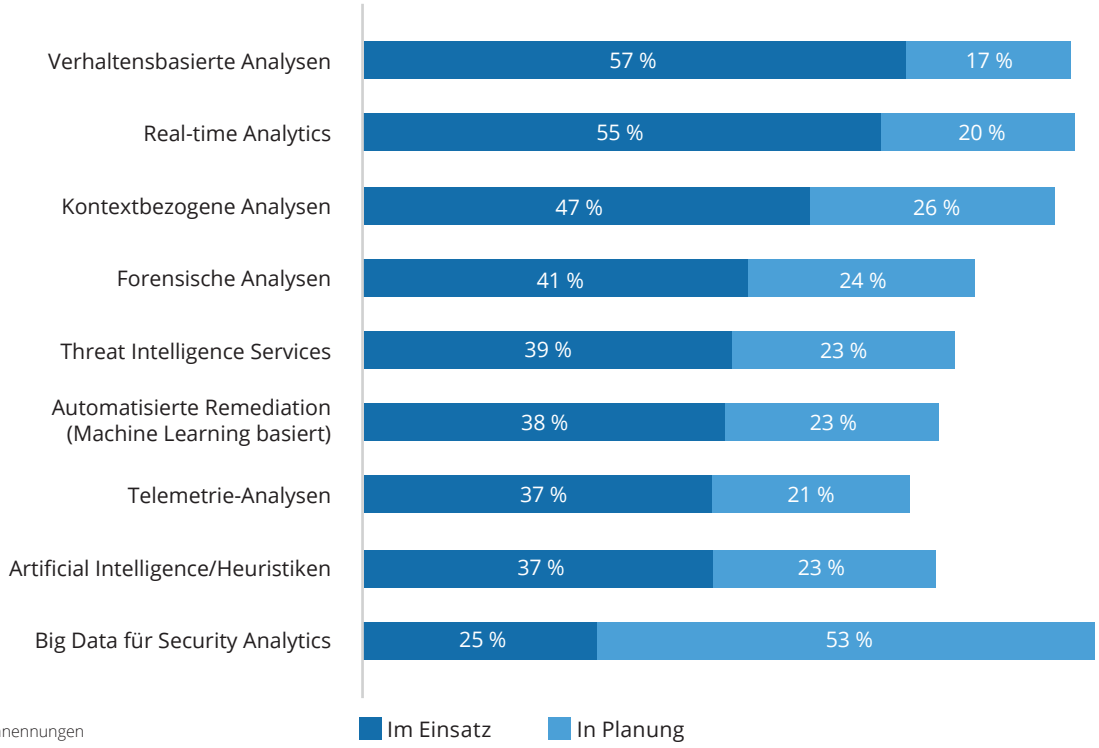
IDC ist davon überzeugt, dass die Bedeutung von Automatisierung und Integration in den kommenden Jahren stark an Bedeutung gewinnen wird, um Prozessketten zu schließen, Security-Silos aufzulösen, Abläufe zu beschleunigen und die Transparenz zu erhöhen.

Analytics und Machine Learning stärken Schutzmechanismen im Vorfeld, da auf Basis von selbstlernenden Systemen unbekannte Aktivitäten schneller erkannt, analysiert und abgewehrt werden

Ratschlag 4: Nutzen Sie unterschiedliche Lösungen und Bereitstellungsmodelle

Die Lösungsbasis und die technologischen Ansätze im Umfeld von Security haben sich in den vergangenen Jahren umfassend weiterentwickelt. Diese Technologien setzen stark auf eine proaktive Überwachung. Analytische Ansätze, die bereits seit einigen Jahren in Security-Lösungen integriert sind, werden seitens der Anbieter als Big Data Security, Künstliche Intelligenz und Machine Learning vermarktet. Analytische Technologien verfügen heute über eine ausreichende Reife und sollten zwingend zu Ihrem Toolset gehören. Investieren Sie also gezielt in Analytics, da sich die Technologie rasch weiterentwickelt und immer besseren Schutz bietet. Kombinieren Sie klassische Lösungsansätze mit aktiven analytischen Überwachungs- und Erkennungs-Tools, um Auffälligkeiten in Echtzeit zu identifizieren und rechtzeitig reagieren zu können. Damit sind Sie in der Lage, Ihre IT-Landschaft robuster gegen Angriffe von innen und außen zu machen und somit den Datenschutz und die Datensicherheit zu erhöhen.

Abbildung 5: Welche analytischen Security-Ansätze nutzen Sie bzw. planen Sie zu nutzen?



N = 230, Mehrfachnennungen

Bei der Evaluierung aktueller Ansätze sollten Sie Security aus der Cloud immer als eine Option betrachten. Zwei Drittel der Unternehmen setzen auf Security aus der Cloud, am häufigsten für Firewall/IDS/IPS, E-Mail-Schutz, Web-Filtering sowie Client-Verwaltung. Security aus der Cloud eignet sich zudem sehr gut zum Schutz mobiler Arbeitsplätze. Nach Meinung von IDC werden cloudbasierte Security-Services in den nächsten Jahren weiter wachsen, da ohne sie praktisch kein Echtzeit-Schutz möglich ist.

Security-Lösungen aus der Cloud werden von zwei Dritteln der befragten Unternehmen genutzt

Ratschlag 5: Entwickeln Sie eine Security-Kultur in Ihrem Unternehmen

IT-Security hat in vielen Unternehmen einen schweren Stand. Sie wird entweder vorausgesetzt, als Bremser im geschäftlichen Alltag verortet oder als notwendiges Übel und lästige Pflicht betrachtet. Das ist eine unbefriedigende IST-Situation. Das bloße Aufstellen von Richtlinien oder Verboten greift zu kurz und kommt bei den Anwendern einfach nicht an. Gehen Sie neue, kreativere Wege, um alle Mitarbeiter für den sicheren Umgang mit mobilen Endgeräten, Apps und Daten zu sensibilisieren. An Ideen mangelt es hier nicht. Live-Hacks, gefakte Phishing-Mails und Penetration Tests können ebenso wie eine Incentivierung für besonders auf Sicherheit bedachte Mitarbeiter erfolgversprechende Maßnahmen sein.

Sensibilisieren Sie gemeinsam mit der Unternehmensführung und den Fachverantwortlichen die Mitarbeiter Ihres Unternehmens für die Rolle von IT-Security für den sicheren Geschäftsbetrieb im digitalen Zeitalter. Denn nur eine hohe Informationssicherheit schützt die Daten, das geistige Kapital und letztendlich das Image und den Ruf, den sich Ihr Unternehmen erarbeitet hat.

FAZIT

Die aktuelle Studie zeigt – wie auch schon die letztjährige – deutlich, dass viele Organisationen immer noch unzureichend geschützt sind. Zwar sind ein Basisschutz und Standard-Security-Lösungen in allen Organisationen vorhanden. Das allein reicht aber allenfalls aus, um großflächig angelegte, tagtäglich gefahrene Standardangriffe abzuwehren. Die umfassende Absicherung der IT-Systeme vor dem Hintergrund der digitalen Transformation bleibt nach wie vor eine der größten Herausforderungen für deutsche IT-Organisationen. Allerdings ist eine weitgehend geschlossene Security-Kette nur in wenigen der befragten Unternehmen vorhanden.

Viele Unternehmen drehen an einzelnen Stellschrauben, betrachten die Thematik aber nicht holistisch. Klar sein dürfte, dass Technologie allein nicht sicher macht. Ein Gesamtlösungsansatz zur Informationssicherheit ist eine Grundvoraussetzung, um alle Komponenten, Lösungen und Prozesse zu erfassen und in der Folge die erforderlichen Richtlinien abzuleiten. Stellen Sie die Verringerung der Komplexität in den Mittelpunkt Ihrer Security-Konzepte. Mittelfristig ist es unabdingbar, dass Sie die klassischen IT-Security-Silos überwinden und Integration und Automatisierung von Security-Prozessen stärker nutzen.

Es zeichnen sich zudem bereits neue Herausforderungen und Veränderungen im Bereich der IT-Sicherheit ab, denen Sie sich stellen müssen. Aus Sicht von IDC werden eine zunehmende Autonomie der Fachbereiche, neue Use Cases jenseits der betriebswirtschaftlichen IT sowie Internet-of-Things-Szenarien verstärkt in den Fokus rücken. Für IT-Entscheider wird es also auch in Zukunft nicht einfacher, das Spannungsfeld aus Business Enablement und sicherem IT-Betrieb aufzulösen.


IDC
ANALYZE THE FUTURE
ONLINE STATISTIC
PROFILE-75N-432
PROFILE-64M-884
PROFILE-251-543
PROFILE-YPD-853
PRODUCT
$820.51
$697.98
$678.06
$507.74
$455.59
$316.40
$284.48
$197.22
$192.19
$116.63

EMPFEHLUNGEN VON ANWENDERN FÜR ANWENDER

Die Befragungsteilnehmer wurden gebeten, anderen Entscheidungsträgern ihre Best Practices im Kontext IT-Sicherheit mitzuteilen. Einige der Antworten sind nachfolgend ungefiltert wiedergegeben. Auf eine Kommentierung wird hier bewusst verzichtet, um einen authentischen Eindruck zu vermitteln.

„Die Umsetzung der DSGVO war bei uns Anlass für weitreichende Maßnahmen."

„Technologien und Lösungen müssen auf dem neusten Stand gehalten werden."

„Wir haben unsere Server gehärtet."

„Wir haben Managed Endpoint Protection unternehmensweit eingeführt. Das hat sich bezahlt gemacht."

„IoT erhöhte die Gefahr durch Fremdeinwirkungen. Planen Sie hier genau."

„Digitalisierung und Cybersecurity erfordern die Ausarbeitung und Umsetzung neuer Konzepte. Da ist ausführliche Beratung sinnvoll, weil man nicht alles selbst wissen kann."

„Die Automatisierung der Sicherheitssysteme und die automatisierte Überwachung ist auf jeden Fall sinnvoll."

„Sicherheitsaspekte und Mitarbeiteranforderungen sollten in Einklang gebracht werden, ohne die Arbeitsfähigkeit des Unternehmens zu gefährden."

„Die Zunahme externer Sensorik macht unsere Systeme offener für externe Bedrohungen. Hier muss man gegensteuern."

„Durch die steigende Komplexität ist der Faktor Mensch ebenfalls eine steigende Fehlerquelle."

„Koordinierte IT-Security-Plattformen und -Standards sind wichtig."

„Es ist in den Köpfen der (meisten) Mitarbeiter angekommen, welche Risiken bestehen."

„Wir haben Daten in die Cloud verlagert und hoffen, dass sie dort sicherer sind als bei uns."

METHODIK

Ziel der im Juni 2018 unter IT- sowie Security-Verantwortlichen durchgeführten Befragung war es, Einblicke in die Pläne, Herausforderungen und Erfolgsfaktoren von deutschen Unternehmen bei der Absicherung der Unternehmens-IT zu erhalten.

Vor diesem Hintergrund hat IDC 230 Verantwortliche aus Unternehmen mit mehr als 20 Mitarbeitern in Deutschland befragt. 58 Prozent der Unternehmen haben zwischen 20 und 1.000 Mitarbeiter und 42 Prozent haben mehr als 1.000 Beschäftige.

Die nachfolgenden Informationen wurden von Matrix42 zur Verfügung gestellt. Für diese Angaben übernimmt IDC keine Gewähr.

IDC
ANALYZE THE FUTURE

MATRIX42

Unternehmensprofil

MATRIX42

WWW.MATRIX42.COM

INFORMATIONEN ZUM UNTERNEHMEN

Matrix42 unterstützt Organisationen dabei, die Arbeitsumgebung ihrer Mitarbeiter zu digitalisieren. Die Software für Digital Workspace Experience verwaltet Geräte, Anwendungen, Prozesse und Services einfach, sicher und konform. Die innovative Software integriert physische, virtuelle, mobile und cloudbasierte Arbeitsumgebungen nahtlos in vorhandene Infrastrukturen. Mit der Übernahme von EgoSecure vervollständigt Matrix42 das Portfolio für Endpoint Security um Funktionalitäten wie Datenverschlüsselung, Schnittstellen- und Applikationskontrolle sowie Security Monitoring. In diesem Bereich konnte EgoSecure 13 Jahre Entwicklungserfahrung sammeln und einen internationalen Kundenstamm etablieren.

POSITIONIERUNG VON IT-SECURITY

Über 70 Prozent der Angriffe im Netzwerk finden auf Endgeräten statt. Darüber hinaus ist der Endpoint die einzige Stelle, an der Daten überhaupt entstehen und zunächst unverschlüsselt vorliegen, sodass die Analyse und der zuverlässige Schutz genau dort ansetzen müssen.

Mit EgoSecure Data Protection bietet Matrix42 eine Komplettlösung für Endpoint Security, die mit sämtlichen Sicherheitsfeatures ausgestattet ist. Dabei werden Endgeräte ganzheitlich und automatisiert geschützt, ohne den Arbeitsfluss zu stören oder die Performance zu verringern. Die Software ist „made in Germany", konform mit den geltenden Anforderungen des Datenschutzes und berücksichtigt dabei die Kontrollfunktion von Betriebsräten.

Darüber hinaus ergänzt der strategische Technologie-Partner enSilo das Produktportfolio mit Post Infection Protection, einer Strategie, die die Ausbreitung von Schadsoftware zuverlässig verhindert, nachdem sie eingedrungen ist.

DARSTELLUNG DES IT-SECURITY-PORTFOLIOS

Das Produktportfolio umfasst folgende Module:

ACCESS CONTROL: Ermöglicht die Kontrolle und Steuerung der Zugriffe auf Geräte und Schnittstellen der Clientumgebung und verhindert so risikobehaftete Datenflüsse. Darüber hinaus werden Daten blockiert, die im Unternehmen nichts verloren haben.

AUDIT: Die Protokollierung der Datenflüsse macht Verstöße gegen Gesetze und Bestimmungen nachweisbar und sorgt für einen bewussten Umgang mit Daten.

DATA LOSS PREVENTION: Daten, die das Know-how des Unternehmens darstellen und/oder als vertraulich eingestuft werden, können das Unternehmen nicht verlassen.

APPLICATION CONTROL: Steuert, welche Anwendungen am Endpoint ausgeführt werden dürfen und welche nicht.

ANTIVIRUS: Bietet neben einer klassischen Antivirus-Funktionalität auch eine Post Infection Protection, um vorhandene Viren zu blockieren.

NEXT GEN ANTIVIRUS: Nutzt Machine Learning und Künstliche Intelligenz, um „Zero Day Exploits" zu erkennen und unschädlich zu machen. Stoppt Schadsoftware vor der Infektion.

Die Datenverschlüsselung sichert Daten auch außerhalb eines Netzwerks und schützt sie so im Fall eines fahrlässigen Datenverlusts oder vorsätzlichen Diebstahls. Hierzu werden folgende Verschlüsselungsmodule geboten:

- **REMOVABLE DEVICE ENCRYPTION** zur Verschlüsselung von Daten auf externen Speichermedien, wie z. B. USB-Sticks
- **CLOUD ENCRYPTION** zur Verschlüsselung von Daten in Cloud-Speichern
- **NETWORKSHARE ENCRYPTION** zur Verschlüsselung von Netzwerkordnern
- **FOLDER ENCRYPTION** zur Verschlüsselung lokaler Verzeichnisse
- **FULL DISK ENCRYPTION** mit Pre-Boot-Authentifizierung (PBA) zur Verschlüsselung von Festplatten, auch bei Ausbau oder Umgehung der Windows-Anmeldung
- **ENCRYPTION ANYWHERE** für iOS und Android, damit der Zugriff auf verschlüsselte Daten auch mobil möglich ist
- **MAIL ENCRYPTION** zur sicheren Gestaltung der E-Mail-Kommunikation

Die Ausarbeitung eines situationsgerechten Schutzkonzeptes ist nur dann möglich, wenn die Gesamtsituation erfasst und richtig eingeschätzt wird. Hierfür liefert INSIGHT ein komplettes Bild aller sicherheitsrelevanten Prozesse und Vorgänge auf dem Endgerät. Die Wirksamkeit kann so regelmäßig überprüft und optimiert werden.
Das Erfassen statistischer Daten über INSIGHT erlaubt es, Anomalien und verdächtiges Verhalten zu erkennen. Das Automatisierungstool INTELLACT leitet basierend auf diesen Daten die nötigen Schutzmaßnahmen ohne menschliches Eingreifen automatisch ein.

Alle Module interagieren untereinander, nutzen eine Datenbank, einen Server, eine Management-Konsole und einen Agenten, sodass Daten nicht doppelt gepflegt werden müssen und die Schutzmechanismen aufeinander abgestimmt sind. Die Module können auch einzeln oder in beliebigen Kombinationen eingesetzt werden. Die Lösung ist multimandantenfähig und erlaubt auch die Verwaltung von Endgeräten, die sich nicht im lokalen Netzwerk befinden.

Interview mit Sergej Schlotthauer, Geschäftsführer bei EgoSecure und Vice President Security bei Matrix42

IT-SECURITY IN DEUTSCHLAND 2018

Anlässlich der Vorstellung der Ergebnisse der Studie „IT-Security in Deutschland 2018" sprach IDC mit Sergej Schlotthauer, Geschäftsführer bei EgoSecure und Vice President Security bei Matrix42.

IDC: Wo liegen für Unternehmen derzeit die größten Herausforderungen im Kontext IT-Security?

Sergej Schlotthauer: Zum einen ist es das mangelnde Wissen. Mitunter fehlt Organisationen noch das Verständnis, dass ein Antivirus-System und eine Firewall zwar notwendig, aber auf keinen Fall ausreichend sind, um Daten zu schützen und DSGVO-compliant zu sein. Zum anderen wird die DSGVO-Thematik zudem meistens sehr stark aus dem organisatorischen und administrativen Blickwinkel betrachtet, dabei wird der technische Teil meistens nicht ausreichend gelöst. Oft liegt der Fokus nur darauf, den Zugriff auf Daten zu beschränken, was nur der erste Schritt von vielen ist. Die Protokollierung des Zugriffs und vor allem die Verschlüsselung der Daten sind meistens nicht ausreichend umgesetzt, obwohl die DSGVO hier klare Vorgaben macht.

Hinzu kommt, dass die aktuelle und zukünftige Sicherheitslage oftmals unterschätzt wird. Die Komplexität des Managements von Arbeitsumgebungen steigt, weil auch Anzahl und Art der Angriffe steigen. Hatte man es vor einigen Jahren mit einigen Einzeltätern und dabei meistens mit Amateuren als Angreifer zu tun, ist Datendiebstahl mittlerweile ein sehr lukratives Geschäft geworden, an dem sich viele extrem professionelle Organisationen, denen beachtliche Ressourcen zur Verfügung stehen, beteiligen. Darüber hinaus kommt es häufig vor, dass Organisationen zögern, die notwendigen IT-Security-Systeme zu implementieren, aus Angst, dass diese die Produktivität der Mitarbeiter verschlechtern.

IDC: Viele Organisationen betrachten IT-Security vorrangig als IT-Thema. Wie bewerten Sie diese Sichtweise?

Schlotthauer: IT-Security muss ganzheitlich betrachtet werden! Das Bewusstsein dafür sowohl beim Management, in Fachabteilungen als auch beim Anwender ist unabdingbar. Trotzdem spielt hier die IT eine tragende Rolle, denn man kann zwar alle im Unternehmen sensibilisieren, aber Fehler nie ganz verhindern. Große Sicherheit schafft hier ein automatisiertes Security Management, das Daten sowohl gegen Vorsatz als auch gegen Fehler schützt und dabei – sei es bewusst oder unbewusst – nicht umgangen werden kann.

IDC: Welche sind die drei wichtigsten Faktoren, die IT-Entscheider unbedingt bei der Absicherung ihrer IT-Umgebung berücksichtigen müssen?

Schlotthauer: Ein wichtiger Faktor ist die Anschaffung eines ganzheitlichen Systems. Es gibt kein einzelnes Feature, das alle Bedrohungen eliminiert. Das kann nur eine Kombination von mehreren, miteinander agierenden und vor allem automatisierten Systemen leisten. Ein weiterer wichtiger Faktor ist die Implementierung eines sozusagen unsichtbaren Systems. Idealerweise können Mitarbeiter mit der richtigen Security-Lösung genauso reibungslos arbeiten wie zuvor, nur sicherer. Zudem muss in ein konformes System investiert werden. Das System muss geltende Gesetze berücksichtigen und auch die Zustimmung des Betriebsrates erlangen.

IDC: Anbieter aus verschiedenen Bereichen adressieren den IT-Security-Markt. Warum ist der Background Ihres Unternehmens die richtige Wahl für Security-Verantwortliche?

Schlotthauer: Matrix42 unterstützt seit mehr als 25 Jahren Organisationen dabei, die Arbeitsumgebung von Mitarbeitern zu digitalisieren. Mit unserer Software können Organisationen Geräte, Anwendungen, Prozesse und Services einfach, sicher und konform verwalten. 2017 sind wir über eine Technologie-Allianz mit dem Security Start-up enSilo in den Markt für Endgerätesicherheit eingestiegen. Mit der Übernahme von EgoSecure vervollständigen wir nun unser Portfolio für Endpoint Security um Funktionalitäten wie Datenverschlüsselung, Schnittstellen- und Applikationskontrolle sowie Security Monitoring.

Wir sind der einzige deutsche Anbieter, der seinen Klienten eine Endpoint-Security-Lösung mit über 15 Modulen aus einer Hand anbietet. Diese Module sind aufeinander abgestimmt und ergänzen sich, funktionieren aber auch alleine oder in Kombination mit anderen. Wir setzen uns klar von weiteren Anbietern ab, die meist nur ein Modul selbst erschaffen haben und ihr Portfolio mit zugekauften Elementen dritter Hersteller erweitern, welche dann gar nicht oder nur rudimentär weiterentwickelt werden.

Unser Ziel ist es, unseren Kunden und deren Anwendern eine IT-Security-Lösung anzubieten, die die Produktivität nicht einschränkt und unbemerkt im Hintergrund läuft. Mit unserer Lösung bieten wir absolute Transparenz über alle sicherheitsrelevanten Vorgänge sowie automatisches Erkennen, Reagieren und Handeln beim Auftreten von Anomalien.

IDC: Werfen wir einen Blick voraus: Worauf müssen Unternehmen langfristig achten, um unnötige Gefährdungen zu vermeiden?

Schlotthauer: Die Bedrohungen werden immer ausgeklügelter und den Angreifern stehen zurzeit enorme Ressourcen zur Verfügung. Nur durch ein mehrschichtiges Schutzsystem, das aufeinander abgestimmte Maßnahmen koordiniert zur Verfügung stellt, volle Transparenz anbietet und automatisiert schützt, sind Organisationen auch in der Zukunft gut gegen Angriffe gewappnet.

Sergej Schlotthauer
Geschäftsführer bei EgoSecure und Vice President Security bei Matrix42

IDC CENTRAL EUROPE GMBH

Hanauer Landstr. 182 D
60314 Frankfurt • Germany
T: +49 69 90502-0
F: +49 69 90502-100
E: info_ce@idc.com
www.idc.de

IDC
ANALYZE THE FUTURE