Vulnerability Management

Wie Unternehmen mit Security-Risiken durch Schwachstellen umgehen

Unterstützt durch

baramundi
Empower your IT

30 YEARS ANNIVERSARY
techconsult
TECHNOLOGY MARKET ANALYSTS

Inhalt

Einleitung

Für viele Unternehmen gehören eine effiziente IT-Infrastruktur und reibungslos funktionierende IT-Prozesse bereits zu den erfolgskritischen Faktoren. Nicht zuletzt durch die pandemiebedingten Veränderungen stehen IT-Verantwortliche vor der großen Herausforderung, diese IT-Architekturen jederzeit mit der höchstmöglichen Leistung und der notwendigen IT-Security bereitstellen zu müssen. Moderne und sich verändernde Arbeitsplatzmodelle streuen zudem die ans Unternehmensnetzwerk angebundenen Endgeräte über Standorte hinweg und führen dazu, dass die Verwaltung der eingesetzten Devices durch die IT-Verantwortlichen immer schwerer wird. Dieser standortübergreifende Einsatz von Geräten kann zudem das Aktualisieren der Systeme und das Entdecken von Schwachstellen erschweren, wenn die Geräte nicht durch die IT-Abteilung verwaltet und über die Entfernung entsprechend aktualisiert werden.

Um eine proaktive IT-Security-Strategie umsetzen zu können, müssen Unternehmen automatisierte Systeme einsetzen, um Risiken und Schwachstellen frühzeitig zu entdecken bzw. zu schließen, bevor diese von Kriminellen ausgenutzt werden. Dazu eignen sich insbesondere Schwachstellenmanagement-Lösungen, um bekannte technische Schwachstellen, Fehlkonfigurationen oder Anomalien in den IT-Systemen zu erkennen und entsprechende Maßnahmen zu ergreifen. Die vorliegenden Ergebnisse machen deutlich, dass die IT-Abteilungen einen routinierten Umgang mit Schwachstellen pflegen, an einigen Stellen jedoch große Lücken bei der Überwachung der Systeme bestehen. So sind den Verantwortlichen Gruppen von IT-Assets im Unternehmen bekannt, die besonders anfällig für Schwachstellen sind, jedoch nicht lückenlos überwacht und verwaltet werden.

Doch welche IT-Assets sind im Unternehmen besonders gefährdet und welche werden von den IT-Verantwortlichen vernachlässigt? Und wie müssen Unternehmen ihren Umgang mit Schwachstellen ändern, um die ganzheitliche Security ihrer IT-Systeme gewährleisten zu können? Welche Kriterien sind für die Verantwortlichen besonders wichtig, wenn es um den Einsatz von Vulnerability Management Software geht? Diese und weitere Fragen werden im Rahmen der vorliegenden Studie untersucht und vorgestellt. Dazu wurden die Antworten von 198 deutschen IT-Verantwortlichen aus Unternehmen mit 100 und mehr Mitarbeitern ausgewertet und im Detail analysiert.

Netzwerkgeräte besonders gefährdet

Um die am Unternehmensnetzwerk angebundenen IT-Assets abzusichern, setzen IT-Verantwortliche immer häufiger auf spezielle Softwarelösungen. So werden in 39 Prozent der befragten Unternehmen Schwachstellenmanagement-Softwarelösungen eingesetzt und die entsprechende Analyse der IT-Systeme und -Assets automatisiert durchgeführt. Darüber hinaus wird in mehr als einem Drittel der Unternehmen (37 Prozent) das Schwachstellenmanagement durch modulare Komponenten der eingesetzten Security-Lösung durchgeführt. Dies hat den Vorteil, dass für IT-Verantwortliche kein zusätzlicher administrativer Aufwand durch neue Softwarelösungen entsteht und die Schwachstellenanalyse direkt aus der bestehenden Security-Lösung gesteuert werden kann.

Rund ein Viertel (24 Prozent) der Unternehmen setzt keine Schwachstellenmanagement-Lösungen ein

Die Relevanz der proaktiven Schwachstellenscans zeigt sich auch bei der Planung des Einsatzes derartiger Lösungen. So geben rund 19 Prozent der befragten IT-Verantwortlichen an, aktuell keine entsprechenden Lösungen einzusetzen, jedoch die Anschaffung innerhalb der nächsten 12 Monate zu planen. Lediglich fünf Prozent der Unternehmen setzen keine derartige Lösung ein und planen dies auch nicht.

Durch unentdeckte IT-Sicherheitslücken könnten Angreifer nicht nur auf das Unternehmensnetzwerk zugreifen, sondern auch geschäftskritische Workflows beeinträchtigen und enorme Schäden verursachen. In Anbetracht dieser potenziellen Risiken müssen Unternehmen eine proaktive Security-Strategie anstreben. Dazu gehört es, insbesondere jene IT-Assets besonders im Fokus zu haben, die am meisten gefährdet sind. Für 44 Prozent der befragten IT-Verantwortlichen sind hierbei die Netzwerkgeräte im Unternehmen mit dem höchsten Risiko behaftet. Denn fehlerhafte Sicherheitskonfigurationen oder Freigaben können, wenn sie unentdeckt bleiben, zu erfolgreichen Cyberangriffen führen. Darüber hinaus sehen 42 Prozent der befragten IT-Verantwortlichen Datenbanken als gefährdet an. So müssen eingesetzte Datenbanksysteme hinsichtlich der Aktualität, häufiger Schwachstellen, unsicherer Passwörter und Standardkonten geprüft werden, um die Kompromittierung von Daten zu verhindern. Damit einhergehend zählen für 40 Prozent der Verantwortlichen die Server- und Desktop-Betriebssysteme ebenfalls zu den gefährdeten IT-Assets im Unternehmen. Insbesondere bei den eingesetzten Betriebssystemen müssen Unternehmen Anfälligkeiten identifizieren und vorhandene Patches zeitnah einpflegen.

Die gefährdetsten IT-Assets aus Sicht der Unternehmen

Basis: 198 Unternehmen, Mehrfachnennungen möglich

Unternehmen haben viele Schwachstellen nicht im Blick

Trotz der hohen wahrgenommenen Gefährdungslage bei den IT-Assets sind viele Unternehmen noch nicht in der Lage, diese ausreichend zu schützen. So hat ein Drittel (33 Prozent) der Unternehmen Schwachstellen bei Cloud-Diensten und -Anwendungen am wenigsten im Überblick.

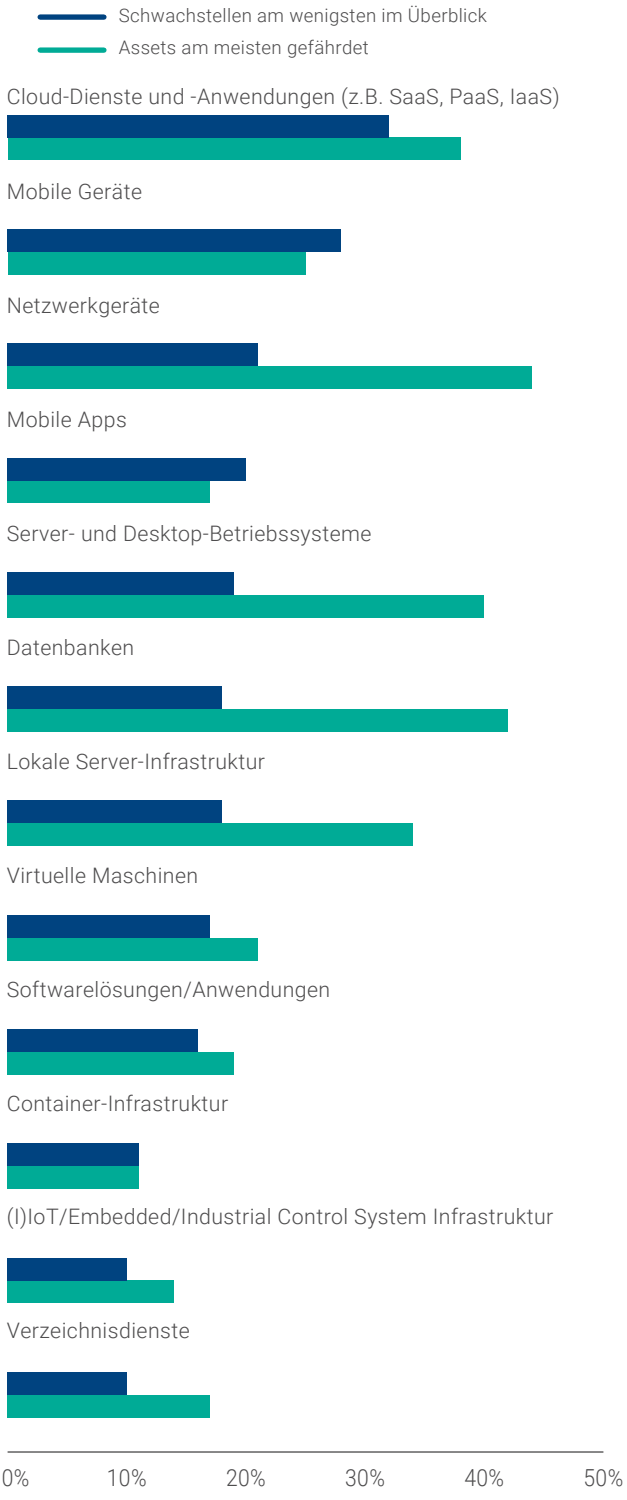
Auch bei lokal oder remote eingesetzten mobilen Endgeräten lassen sich potenzielle Gefahren identifizieren. So hat deutlich mehr als ein Viertel (28 Prozent) der befragten IT-Verantwortlichen mögliche Schwachstellen von mobilen Devices und 20 Prozent von mobilen Apps am wenigsten im Überblick. Nicht zuletzt durch die pandemiebedingten Änderungen gehören mobile Endgeräte wie Tablets oder Laptops zu gängigen Arbeitsmitteln von Mitarbeitern, weshalb diese Geräte besonders im Fokus der Security-Bemühungen stehen sollten. Dazu müssen Informationen zu den Endgeräten und zum Versionsstand der Betriebssysteme erfasst werden, um den Sicherheitsstatus und mögliche Aktualisierungsbedarf zu prüfen.

Unternehmen haben Schwachstellen von Cloud-Anwendungen (29 Prozent) und mobilen Endgeräten (28 Prozent) am wenigsten im Überblick

Besonders akuter Handlungsbedarf lässt sich bei der Verwaltung von Netzwerkgeräten erkennen. So werden diese zwar mit einem hohen Gefahrenpotential bewertet, jedoch haben 21 Prozent der Unternehmen die Schwachstellen derartiger Geräte am wenigsten im Überblick. Dadurch können unentdeckte Schwachstellen durch bspw. fehlerhaft eingestellte Standardkonfigurationen langfristig ein großes Sicherheitsrisiko für die Unternehmens-IT darstellen. Für IT-Verantwortliche ist es somit unabdingbar, automatisierte Tools zur Verwaltung von Sicherheitskonfigurationen aller relevanten Geräte und Systeme einzusetzen. Nur so können Schwachstellen frühzeitig identifiziert und geschlossen werden.

Einschätzung der Gefährdung und Absicherung von IT-Assets

Basis: 198 Unternehmen



Umgang mit Schwachstellen

Für das Schwachstellenmanagement sind oftmals unterschiedliche Mitarbeiter in den Unternehmen primär verantwortlich. So sind in 37 Prozent der befragten Unternehmen die Leiter der IT-Abteilung zuständig für diese Tätigkeit, jedoch auch IT-Mitarbeiter (33 Prozent) sowie IT-Administratoren (27 Prozent). In eher kleineren Unternehmen sind dagegen IT-Security-Mitarbeiter (31 Prozent) zuständig für das Schwachstellenmanagement, wohingegen in größeren Unternehmen häufig die IT-Netzwerkleitung (33 Prozent) die Verantwortung für diese Tätigkeit übernimmt.

In 37 Prozent Unternehmen sind die IT-Leiter und in jedem dritten Unternehmen (33 Prozent) die IT-Mitarbeiter zuständig für das Schwachstellenmanagement

Unabhängig von der Zuständigkeit müssen Unternehmen bereits im Vorfeld den Umgang mit identifizierten Schwachstellen definieren. Mehr als jedes zweite Unternehmen (53 Prozent) geht dabei systematisch vor und beseitigt alle gefundenen Schwachstellen. Hierfür müssen Unternehmen über ausreichend Ressourcen verfügen, um die Beseitigung der Schwachstellen durchführen zu können. Denn je komplexer und größer die IT-Infrastruktur ist, desto mehr Sicherheitslücken und Fehlkonfigurationen sind zu erwarten. Sollten Unternehmen jedoch nicht über ausreichend Kapazitäten verfügen, können sie die Schwachstellen auch priorisieren. So werden in 29 Prozent der Unternehmen die identifizierten Lücken zunächst priorisiert und nur die mit dem größten Risiko für die IT-Infrastruktur beseitigt. Beide Vorgehensweisen erfordern softwaregestützte Systeme, die nicht nur die Priorisierung der Schwachstellen, sondern auch Patches, Updates und Konfigurationen durchführen.

13 Prozent der Unternehmen werden erst tätig, wenn Schwachstellen von Kriminellen ausgenutzt werden

Dahingegen verfolgen 13 Prozent der befragten Unternehmen einen reaktiven Ansatz. Dabei werden Schwachstellen nur dann geschlossen, wenn diese im eigenen oder in anderen Unternehmen für Cyberangriffe genutzt wurden. Bei größeren Unternehmen mit 1000 bis 5000 Mitarbeitern liegt dieser Anteil sogar bei 26 Prozent, was in Anbetracht der komplexen IT-Infrastrukturen verständlich erscheint, jedoch große Risiken für das Unternehmen mit sich bringt. In 5 Prozent der befragten Unternehmen wird der Umgang mit Schwachstellen je nach individueller Beurteilung entschieden, ohne eine systematische Vorgehensweise definiert zu haben. Durch diesen personalintensiven Umgang mit Schwachstellen besteht die Gefahr, dass Sicherheitslücken nicht korrekt eingeschätzt oder zu spät behoben werden, was zu einem höheren Risikopotenzial für das Unternehmen führen kann.

In 47 Prozent der Unternehmen werden identifizierte Schwachstellen nicht sofort beseitigt

Insgesamt wird deutlich, dass gut jedes zweite Unternehmen (47 Prozent) nicht jede identifizierte Schwachstelle sofort schließt. Eine proaktive Vorgehensweise mithilfe softwaregestützter Lösungen ist notwendig, um Sicherheitslücken rechtzeitig zu erkennen und zu bewerten. Dazu gehört auch das kontinuierliche Scannen der IT-Infrastruktur, um verwundbare Systeme frühestmöglich zu lokalisieren, zu aktualisieren und so langfristig die Kosten des IT-Betriebs zu senken.

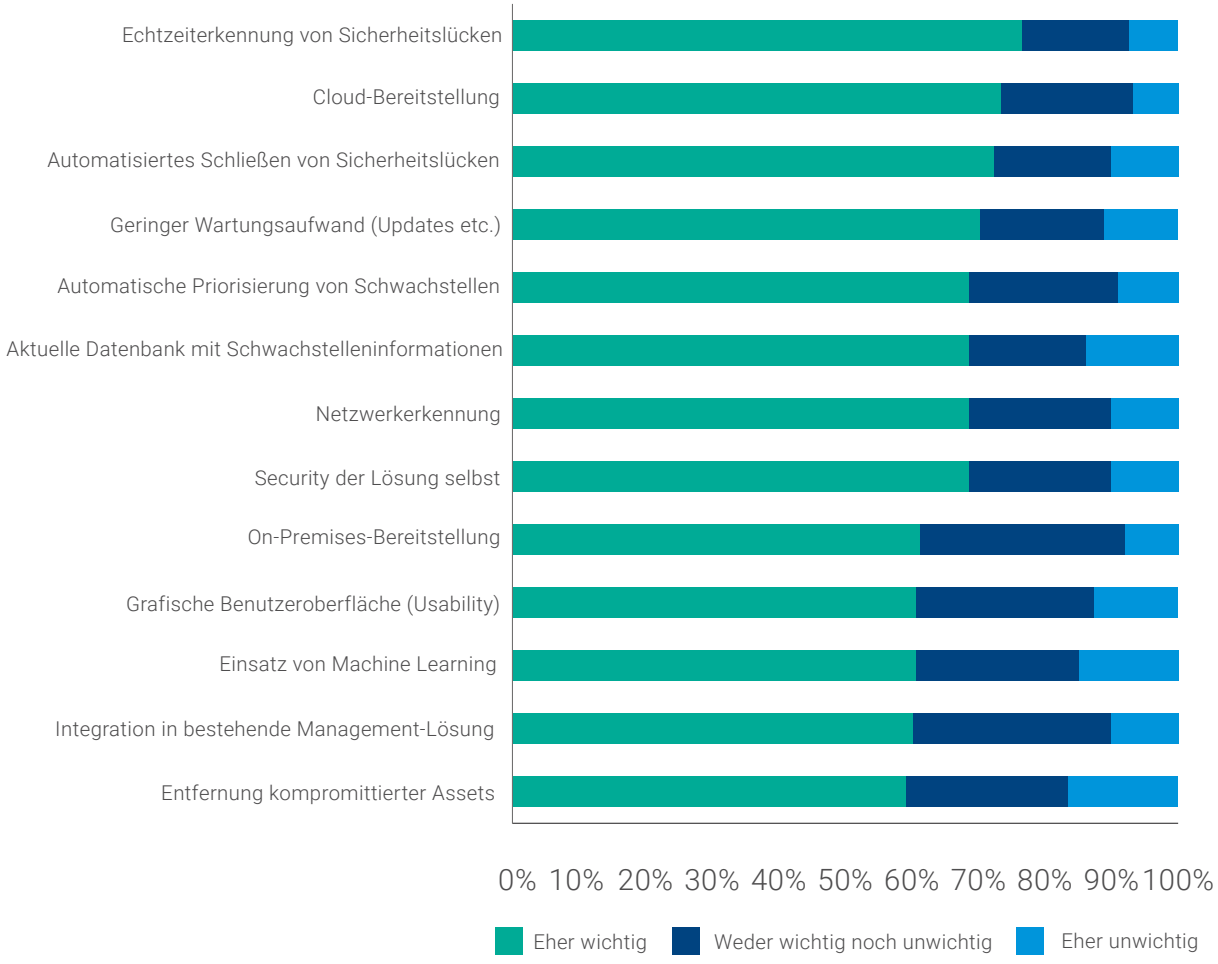
Proaktive Beseitigung von Schwachstellen relevant

Zum softwaregestützten Umgang mit potenziellen IT-Risiken können Unternehmen auf Schwachstellenmanagement-Lösungen zurückgreifen. Dabei wird von mehr als drei Viertel der befragten Unternehmen (77 Prozent) die Echtzeiterkennung von Sicherheitslücken und fehlerhaften Konfigurationen als wichtigstes Kriterium hervorgehoben. Dadurch lassen sich neue Systemupdates, Versionen und Patches ermitteln und Schwachstellen unmittelbar nach ihrer Entdeckung identifizieren und beseitigen. Für 73 Prozent der Befragten spielt zudem die Cloud-Bereitstellung eine maßgebliche Rolle bei der Wahl einer derartigen Lösung sowie für 72 Prozent das automatisierte Schließen von Sicherheitslücken.

Die Funktion des automatischen Schließens von Sicherheitslücken in Kombination mit der Echtzeitüberwachung kann den IT-Abteilungen viel Arbeit abnehmen, denn der Großteil der Schwachstellen lässt sich nicht nur automatisiert erkennen, sondern auch automatisiert beheben. Durch die Bereitstellung einer derartigen Lösung in der Cloud wird die Unternehmens-IT permanent in Echtzeit überwacht. Aus diesem Grund spielen derartige Lösungen insbesondere für gewachsene IT-Infrastrukturen und größere Unternehmen eine maßgebliche Rolle bei der Absicherung ihrer Systeme.

Schwachstellenmanagement-Lösungen - Wichtige Kriterien

Basis: 188 Unternehmen, Unternehmen in denen Schwachstellenmanagement-Lösungen eingesetzt werden



Fazit

Die strategische Ausrichtung der Unternehmen muss zwingend auch eine langfristige IT-Security-Strategie umfassen. Denn nicht nur durch die pandemiebedingten Umstrukturierungen im Arbeitsumfeld sondern auch durch die zunehmende Digitalisierung in Unternehmen können Sicherheitslücken schnell zu Problemen führen und Workflows negativ beeinflussen. Um die Sicherheit der IT-Systeme langfristig gewährleisten zu können, muss deshalb ein proaktiver Umgang mit potenziellen Schwachstellen und Sicherheitslücken angestrebt werden. Nur durch softwaregestützte Überwachung aller relevanten IT-Systeme können diese in Echtzeit geprüft, potenzielle Schwachstellen identifiziert und diese sogar unmittelbar automatisiert behoben werden. Denn nur eine proaktive Vorgehensweise im Umgang mit Sicherheitslücken ist im Einklang mit einer ganzheitlichen Security-Strategie zu sehen. Dies führt langfristig nicht nur zu einer Entlastung der IT-Abteilung, sondern auch zur Kosteneffizienz im IT-Betrieb.

Zur Studie

Im Rahmen der vorliegenden repräsentativen Studie wurden im Juli 2022 insgesamt 201 IT- und Businessentscheider zum Einsatz von Endpoint-Management-Lösungen befragt.

Geschäftsführer, CEO, COO: 5%
IT-Manager/CIO: 25%
IT-Abteilungsleiter/Teamleiter: 32%
Leiter IT-Infrastruktur: 9%
IT-Administrator: 11%
IT-Mitarbeiter: 13%
Andere: 5%

Industrie (34%
Handel (5%)
Dienstleistung (43%)
Banken und Versicherung (4%)
Öffentliche Verwaltungen, Non-Profit, Gesundheits- und Sozialwesen (14%)

Weitere Informationen

Impressum

techconsult GmbH
Baunsbergstraße 37
34131 Kassel

E-Mail: **info@techconsult.de**
Tel.: +49 561 8109 0
Fax: +49 561 8109 101
Web: **www.techconsult.de**

Kontakt baramundi

baramundi software AG
Beim Glaspalast 1
86153 Augsburg

Aufgrund von Rundungsanpassungen summieren sich einige Summen möglicherweise nicht zu 100%.

Aus Gründen der besseren Lesbarkeit wird bei Personenbezeichnungen und personenbezogenen Hauptwörtern in dieser Studie die männliche Form verwendet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

Kontakt

Ercan Hayvali
Analyst
E-Mail: **ercan.hayvali@techconsult.de**
Tel.: +49 561 8109 178

Tel: +49 821 56708 0
Fax: +49 821 56708 19
E- Mail: **request@baramundi.com**
Web: **www.baramundi.com**

Über die techconsult GmbH

Die techconsult GmbH, gegründet 1992, zählt zu den etablierten 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.

Über die baramundi software AG

baramundi ermöglicht Unternehmen und Organisationen weltweit das effiziente, sichere und plattformübergreifende Management von vernetzten Endgeräten im Bereich IT und Manufacturing. Die Management Suite bietet unseren Kunden ein ganzheitliches, zukunftsorientiertes Unified Endpoint Management.

baramundi ist Vorreiter im Bereich des Unified Endpoint Managements der vernetzten Produktion. Diese Lösung entwickeln wir in enger Zusammenarbeit mit dem Digitalization Center von WITTENSTEIN.

Seit zwei Jahrzehnten sind wir bei baramundi die Experten für Unified Endpoint Management. Unsere Management Suite umfasst Client Management, Mobile Device Management und Endpoint Security innerhalb einer Oberfläche und einer einzigen Datenbank.

Die Lösung ermöglicht die Automatisierung von Routinearbeiten, eine umfassende Übersicht über Netzwerk und Endgeräten sowie die Optimierung und Absicherung vernetzter Prozesse: auf (i)PCs, Servern und Notebooks sowie auf Mobilgeräten und Industrial Control Systems (ICS). IT-Verantwortliche werden damit in die Lage versetzt, kontinuierlich den aktuellen Sicherheitsstatus der IT-Infrastruktur zu verfolgen und diese optimal gegen Cyberangriffe zu schützen