CYBERSECURITY SPECIAL REPORT

KLEINE UND MITTELSTÄNDISCHE UNTERNEHMEN

Klein und leistungsstark

Wie kleine und mittelständische Unternehmen ihre Verteidigungslinie gegen aktuelle Bedrohungen stärken können

CISCO

53 % aller mittelständischen Unternehmen waren von einer Sicherheitsverletzung betroffen

Bis zu

5.000

Durchschnittliche Anzahl der Sicherheitswarnungen

Mittelständische Unternehmen untersuchten 55,6 % der Sicherheitswarnungen

29 % aller mittelständischen Unternehmen gaben an, Sicherheitsverletzungen verursachten Kosten von weniger als 100.000 USD. 20 % gaben an, die verursachten Kosten lägen zwischen 1.000.000 und 2.499.999 USD.

Viele kleine und mittelständische Unternehmen streben eine effektivere Cybersicherheit an, ganz ähnlich wie Großunternehmen. KMUs sind dynamisch und unternehmen besondere Anstrengungen, um Innovationen zu schaffen. Sie entwickeln sich schneller und leisten im Verhältnis mehr als Großunternehmen. Gleichzeitig sind sie aber den gleichen Cyberbedrohungen ausgesetzt.

In der heutigen Cyberbedrohungslandschaft ist jedes Unternehmen unabhängig von seiner Größe einem Angriffsrisiko ausgesetzt. Kleine und mittelständische Unternehmen werden jedoch immer häufiger Ziel von Angriffen[1] und dienen dabei als Ausgangspunkt für größere Kampagnen. Die Angreifer halten kleine und mittelständische Unternehmen für weiche Ziele mit weniger anspruchsvollen Sicherheitsinfrastrukturen und -vorkehrungen, die zudem nicht über ausreichend geschultes Personal für die Reaktion auf Bedrohungen verfügen.[1]

Viele kleine und mittelständische Unternehmen beginnen erst zu erkennen, wie attraktiv sie für Cyberkriminelle sind. Diese Erkenntnis kommt jedoch häufig zu spät, nämlich erst nach einem Angriff. Je nach Art und Umfang der Kampagne kann die Schadensbehebung nach einem Cyberangriff für diese Unternehmen schwierig und teuer sein – wenn nicht gar unmöglich. Dieser Bericht verdeutlicht die Risiken für kleinere Unternehmen und gibt Tipps, wie kleinere Unternehmen ihre Sicherheitsvorkehrungen aufrüsten können und was sie 2018 und darüber hinaus bedenken sollten.

Laut der Security Capabilities Benchmark Study 2018 führten mehr als der Hälfte aller Cyberangriffe (54 Prozent) zu finanziellen Schäden von über 500.000 US-Dollar, unter anderem durch den Verlust von Umsätzen, Kunden und Geschäftschancen sowie Out-of-Pocket-Zahlungen. Eine solche Summe kann für ein unvorbereitetes kleines/mittelständisches Unternehmen leicht das Ende bedeuten.

Eine aktuelle Studie des Better Business Bureau (BBB)[2] verdeutlicht ebenfalls die weitreichenden finanziellen Folgen, die ein schwerer Cyberangriff für kleine und mittelständische Unternehmen haben kann. Das BBB fragte die Inhaber kleiner Unternehmen in Nordamerika, wie lange sie ihr Geschäft rentabel weiterbetreiben könnten, wenn sie dauerhaft den Zugriff auf wichtige Daten verlieren würden. Nur etwa ein Drittel (35 Prozent) gaben an, sie könnten länger als drei Monate einen rentablen Geschäftsbetrieb aufrechterhalten. Mehr als die Hälfte erwartete, in weniger als einem Monat nicht mehr rentabel zu arbeiten.

Wir definieren KMUs als Unternehmen mit weniger als 250 Mitarbeitern und mittelständische Unternehmen als solche mit 250 bis 499 Mitarbeitern. Beide Segmente werden in diesem Bericht untersucht.

Wir haben die Erkenntnisse aus den Angaben von KMUs in unserer Security Capabilities Benchmark Study 2018 analysiert (in diesem Bericht kurz als Benchmark-Studie bezeichnet). Die Studie liefert Erkenntnisse zu den aktuell getroffenen Sicherheitsvorkehrungen sowie einen Vergleich aller Ergebnisse mit den letzten drei Jahren.

Wir haben Teilnehmer aus 1.816 KMUs und mittelständischen Unternehmen in 26 Ländern befragt.

1 Cyberthreats and Solutions for Small and Midsize Businesses, Vistage Research Center, 2018. Entwickelt in Zusammenarbeit mit Cisco und The National Center for the Middle Market. Verfügbar unter https://www.vistage.com/research-center/business-operations/risk-management/20180503-22912/.

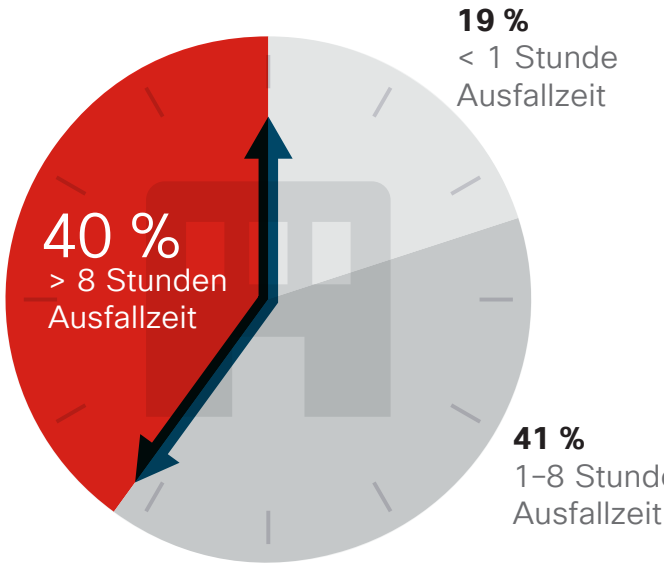
2 2017 State of Cybersecurity Among Small Businesses in North America, BBB, 2017: https://www.bbb.org/globalassets/shared/media/state-of-cybersecurity/updates/cybersecurity_final-lowres.pdf

Welche Folgen kann ein einziger Tag ohne Geschäftsbetrieb für uns schon haben?

Diese Aussage wird man von einem IT-Administrator kaum hören. Systemausfallzeiten beeinträchtigen Produktivität und Rentabilität und sind daher ein erhebliches Problem für Unternehmen nach einem Cyberangriff. Der Benchmark-Studie zufolge verzeichneten 40 Prozent der Befragten (250–499 Mitarbeiter) im vergangenen Jahr infolge einer schweren Sicherheitsverletzung Systemausfallzeiten von acht Stunden oder mehr (Abbildung 1). Ähnliche Ergebnisse ermittelte Cisco im Rahmen der Studie für größere Unternehmen (mit 500 oder mehr Mitarbeitern). Der Unterschied besteht allerdings darin, dass größere Unternehmen nach einem Angriff tendenziell auf eine größere Ausfallsicherheit als kleine und mittelständische Unternehmen zählen können, weil sie über mehr Ressourcen für Reaktion und Wiederherstellung verfügen.

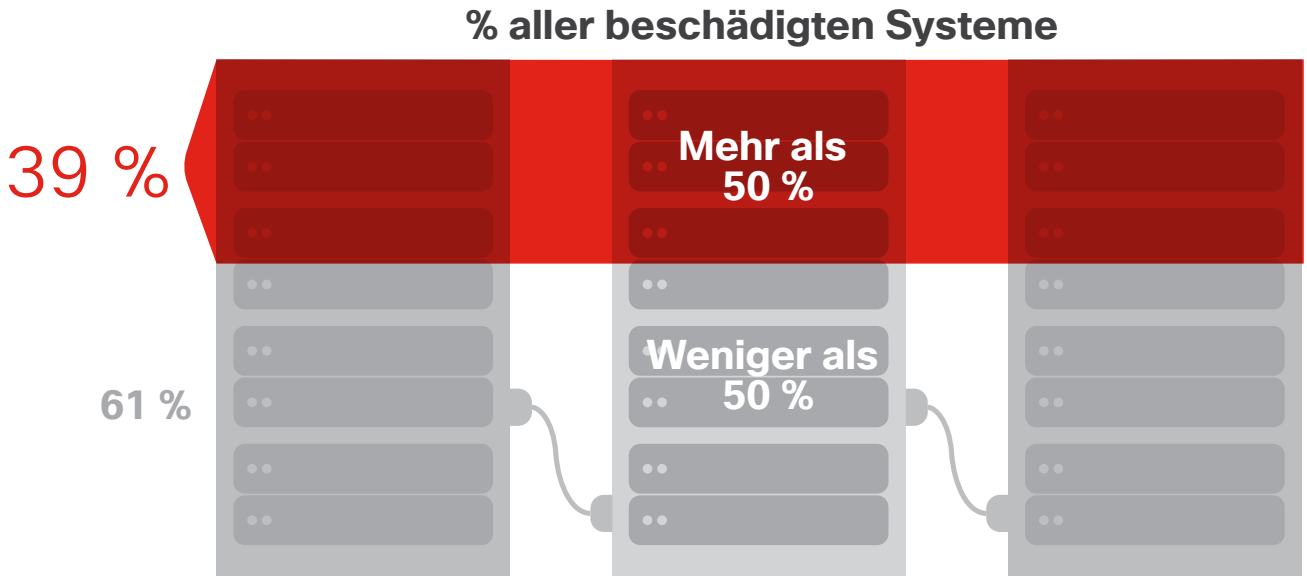
Zudem gaben 39 Prozent der Befragten an, mindestens die Hälfte ihrer Systeme sei von einer schweren Sicherheitsverletzung betroffen gewesen (Abbildung 2). Kleinere Unternehmen unterhalten in der Regel seltener mehrere Standorte oder Geschäftssegmente, und ihre zentralen Systeme sind meist enger miteinander verbunden. Wenn diese Unternehmen angegriffen werden, kann die Bedrohung sich schnell und einfach vom Netzwerk auf andere Systeme ausbreiten.

Abbildung 1: Systemausfallzeiten nach einer schweren Sicherheitsverletzung



Quelle: Cisco Security Capabilities Benchmark Study 2018

Abbildung 2: Anteil der von einer schweren Sicherheitsverletzung betroffenen Systeme



Quelle: Cisco Security Capabilities Benchmark Study 2018

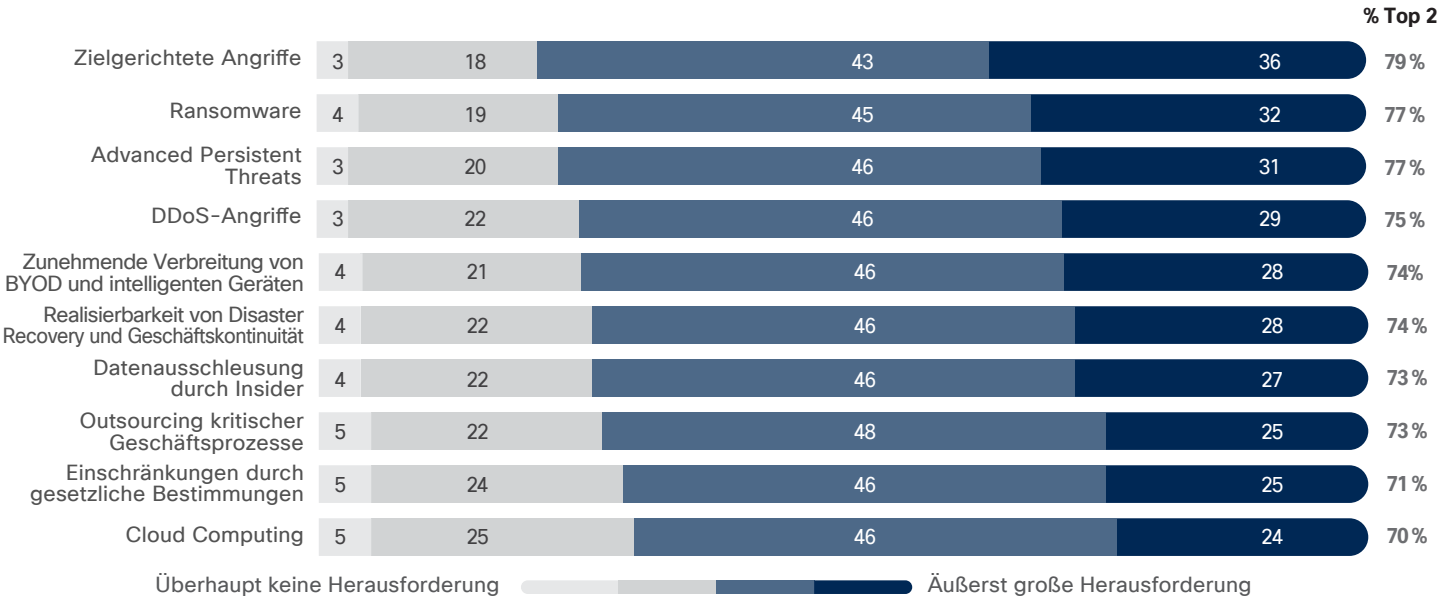
Schlaflose Nächte für Sicherheitsverantwortliche

Auf die Frage nach ihren größten Herausforderungen bei der Sicherheit nannten die Befragten vor allem drei Punkte:

- Zielgerichtete Angriffe auf Mitarbeiter (gut gemachtes Phishing)
- Advanced Persistent Threats (erstmals in Erscheinung tretende fortschrittliche Malware)
- Ransomware

Bei Ransomware (interessanterweise nicht unter den drei größten Herausforderungen von Großunternehmen) handelt es sich, wie Sie inzwischen sicherlich wissen, um Malware, durch die in der Regel Daten verschlüsselt werden, bis die betroffenen Benutzer auf eine Lösegeldforderung eingehen. Für kleine und mittelständische Unternehmen kann dies schwerwiegende Störungen und Systemausfallzeiten zur Folge haben. Ransomware kommt diese Unternehmen aber auch auf andere Weise teuer zu stehen: Wie Sicherheitsexperten von Cisco erklären, sind kleine und mittelständische Unternehmen eher zur Lösegeldzahlung bereit, um den Normalbetrieb schnell wiederaufnehmen zu können. Sie können sich diese Ausfallzeiten und den fehlenden Zugriff auf wichtige Daten – einschließlich Kundendaten – schlicht nicht leisten. (Siehe Abbildung 3.)

Abbildung 3: Wichtigste Sicherheitsbedenken für den Mittelstand[5]



Quelle: Cisco Security Capabilities Benchmark Study 2018

Weitere Bedrohungen, die KMUs nicht ignorieren können

Trotz aller Sorgen stufen die Sicherheitsexperten von Cisco Ransomware als abnehmende Bedrohung ein, da immer mehr Angreifer ihren Schwerpunkt auf das illegale Generieren von Kryptowährungen („Cryptomining“) verlagern. Diese Aktivität ist gleich in dreifacher Hinsicht attraktiv: Sie kann äußerst lukrativ sein, Auszahlungen lassen sich nicht zurückverfolgen, und die Wahrscheinlichkeit ist geringer, dass Angreifer für ihre Handlungen strafrechtlich belangt werden. (So besteht beispielsweise kein Risiko, dass Patienten eine wichtige Behandlung vorenthalten wird, weil die Systeme und wichtigen Daten eines Krankenhauses durch Ransomware gesperrt wurden.) Angreifer können auch Mining-Software durch verschiedene Methoden einschleusen, etwa E-Mail-basierte Spam-Kampagnen oder Exploit-Kits.[3]

3 „Ransom Where? Malicious Cryptocurrency Miners Takeover, Generating Millions“, Cisco Talos-Blog, 31. Januar 2018: https://blog.talosintelligence.com/2018/01/malicious-xmr-mining.html.

Die Sicherheitsforscher von Cisco erläutern, dass Cyberkriminelle mit dem neuen Geschäftsmodell des illegalen Cryptominings „ihre Opfer nicht mehr für das Öffnen eines Anhangs oder das Ausführen eines schädlichen Skripts bestrafen, indem sie Systeme als Geiseln nehmen und ein Lösegeld fordern. Jetzt nutzen [sie] aktiv die Ressourcen der infizierten Systeme aus.“[4] Für kleine und mittelgroße Unternehmen, die ungewollt illegales Cryptomining unterstützen, kann eine geringere Systemleistung der einzige Hinweis auf eine Kompromittierung sein – es sei denn, sie verfügen über die richtige Technologie zur Erkennung solcher Cryptomining-Aktivitäten.

Die Insider-Bedrohung von 0,5 %: 100 % zu viel?

Wenn die befragten Unternehmen immer mehr Daten und Prozesse in die Cloud verlagern, müssen sie auch geeignete Maßnahmen ergreifen, um eine andere potenzielle Bedrohung abzuwehren: böswillige Insider. Ohne Tools zur Erkennung verdächtiger Aktivitäten (z. B. das Herunterladen vertraulicher Kundendaten) riskieren sie den Verlust geistigen Eigentums oder sensibler Finanz- und Kundendaten über die unternehmenseigenen Cloud-Systeme.

Eine kürzlich von den Sicherheitsforschern von Cisco durchgeführte Untersuchung verdeutlicht das Risiko: Von Januar bis Juni 2017 wurden Datendiebstahlstrends mithilfe von maschinellem Lernen untersucht, um 150.000 Benutzer in 34 Ländern zu profilieren, die Cloud-Services nutzen. Innerhalb von 1,5 Monaten ermittelten unsere Forscher, dass 0,5 Prozent der Benutzer verdächtige Downloads tätigten. Ein halbes Prozent ist zu vernachlässigen? Anders ausgedrückt: Zwei Mitarbeiter eines Unternehmens mit 400 Personen sind böswillige Insider. Das sind 100 Prozent zu viel. Insbesondere wurden von diesen Benutzern insgesamt mehr als 3,9 Millionen Dokumente aus den unternehmenseigenen Cloud-Systemen heruntergeladen. Das sind durchschnittlich 5.200 Dokumente pro Benutzer über einen Zeitraum von 1,5 Monaten.[5]

Cisco Security Capabilities Benchmark Study 2018

In diesem Sonderbericht werden ausgewählte Daten und Erkenntnisse aus der Cisco Security Capabilities Benchmark Study 2018 vorgestellt. An der Untersuchung waren mehr als 3.600 Befragte in 26 Ländern beteiligt. Weitere Erkenntnisse zu den aktuell in Unternehmen aller Größen getroffenen Sicherheitsvorkehrungen sowie einen Vergleich mit den Ergebnissen früherer Studien von Cisco finden Sie im *Cisco Annual Cybersecurity Report 2018* unter https://www.cisco.com/c/en/us/products/security/security-reports.html.

4 Ebd.
5 Weitere Informationen finden Sie unter „Insider threats: taking advantage of the cloud“ im Cisco 2018 Annual Cybersecurity Report unter https://www.cisco.com/c/en/us/products/security/security-reports.html.

Herausforderungen

Die beste Verteidigung gegen die zuvor beschriebenen Bedrohungen erfordert eine Koordination und Orchestrierung der IT-Ressourcen. Bei diesen Ressourcen handelt es sich im Allgemeinen um die Menschen, Prozesse und Technologien, die Unternehmen einsetzen können, um Angriffe zu verhindern.

Mehr noch als Großunternehmen müssen kleinere Unternehmen jedoch diese Ressourcen so koordinieren können, dass sie Einblicke in Bedrohungen liefern und Angriffe verhindern oder abwehren können, bevor sie Schaden verursachen. Der fortwährende Mangel an talentierten Sicherheitsfachkräften, von dem auch Großunternehmen betroffen sind, trifft kleinere Unternehmen noch sehr viel mehr.

Sicherheitstechnologietrends in KMUs

In Zukunft werden kleinere Unternehmen versuchen, die Herausforderungen bei der Cybersicherheit mit neuen Tools zu bewältigen, um Bedrohungen zu stoppen.

Die im Rahmen der Benchmark-Studie Befragten gaben an, bei entsprechender Verfügbarkeit ihre personellen Ressourcen wie folgt einsetzen zu wollen:

- Upgrade der Endpunktsicherheit auf fortschrittlicheren erweiterten Malwareschutz – mit 19 Prozent die häufigste Antwort
- Einsatz besserer Sicherheitsmaßnahmen für Webanwendungen gegen webbasierte Angriffe (18 Prozent)
- Bereitstellung von Intrusion Prevention, das nach wie vor als wichtige Technologie zur Abwehr von Netzwerkangriffen und Exploit-Versuchen gilt (17 Prozent) (Siehe Abbildung 5.)

Bei der Bewertung neuer Technologien besteht eine Herausforderung für Unternehmen darin, zu ermitteln, wie gut ihre Sicherheitsprodukte zusammenarbeiten. Der Managementaufwand durch die Beobachtung zahlreicher Konsolen, um auf Bedrohungen oder Sicherheitsverletzungen reagieren zu können, ist nicht zu unterschätzen.

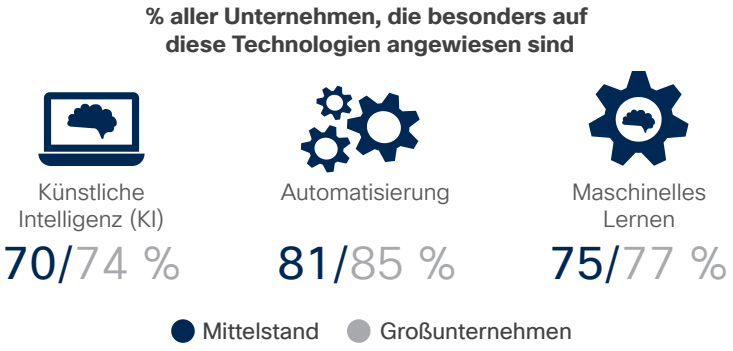
„Viele glauben, sie seien durch einen „Best-of-Breed-Ansatz“ mit mehreren Anbietern besser geschützt“, so Ben M. Johnson, CEO des Cisco Partners Liberty Technology aus Griffin im US-Bundesstaat Georgia. „Tatsächlich stellen wir jedoch fest, dass solche Systeme schwieriger zu managen sind, mehr kosten und die Sicherheitseffektivität insgesamt sogar verringern.“

Maschinelles Lernen und Sicherheit: Hilfe oder Hype?

Der aktuelle Hype rund um maschinelles Lernen ließ sich kaum ignorieren. Wie sich herausstellt, setzen mittelständische Unternehmen in ähnlichem Maße wie größere Unternehmen auf Lösungen für Verhaltensanalysen, die Angriffe effektiv erkennen können. Lösungen, die maschinelles Lernen und Automatisierung nutzen, werden von mittelständischen Unternehmen etwas seltener eingesetzt als von solchen mit mehr als 1.000 Mitarbeitern (Abbildung 4).

Maschinelles Lernen bzw. dessen Lernprozess ist am effektivsten, wenn die Technologie als zusätzliche Erkennungsebene eines bereits bereitgestellten Produkts und nicht als separates Produkt eingesetzt wird. Auf diese Weise profitieren die Teams ohne Mehrbelastung von den Vorteilen des maschinellen Lernens zur Erkennung von Anomalien und Bedrohungen in „Maschinengeschwindigkeit“.

Abbildung 4: Mittelständische Unternehmen sind weniger abhängig von Automatisierung und KI-Tools.



Quelle: Cisco Security Capabilities Benchmark Study 2018

Mobiler Mittelstand

Unternehmen erkennen auch, dass ihre Sicherheitsansätze die Anforderungen der modernen Arbeitsumgebung erfüllen müssen – insbesondere in Bezug auf die zunehmende Mobilität und die Nutzung von Mobilgeräten. 56 Prozent der Befragten gaben an, der Schutz von Mobilgeräten vor Cyberangriffen sei eine sehr große oder äußerst große Herausforderung.

Der Mittelstand und die Cloud

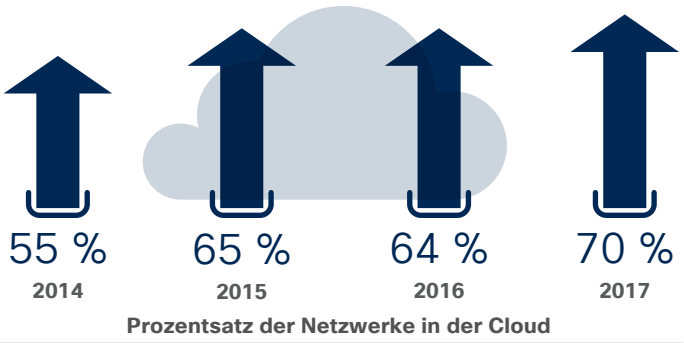
Angesichts ihrer Herausforderungen bei der Sicherheit versuchen viele der Befragten, mithilfe der Cloud ihre Verteidigungslinie zu stärken, ohne die vorhandenen Ressourcen zusätzlich zu belasten. Dabei stellt sich jedoch die Frage, ob die Verlagerung der Sicherheit in die Cloud als Strategie zur Abwehr von Angriffen ausreichend ist. Darüber hinaus können Unternehmen die Verantwortung für die Sicherheit nicht einfach abtreten, indem sie ihre Daten in die Cloud verschieben: Sie müssen dennoch über die Sicherheitskontrollen der Cloud-Anbieter im Bilde sein und zudem wissen, wie potenzielle Sicherheitsverletzungen in der Cloud sich auf lokale Ressourcen auswirken können.

Die Einführung von Cloud-Services ist der Studie von Cisco zufolge in mittelständischen Unternehmen eindeutig auf dem Vormarsch. 2014 gaben noch 55 Prozent dieser Unternehmen an, sie würden einige ihrer Netzwerke in einer Form der Cloud hosten; 2017 waren es bereits 70 Prozent (Abbildung 5).

Viele der Befragten sind der Meinung, die Cloud könne ihnen dabei helfen, bestimmte Lücken in ihrer Verteidigungslinie zu schließen und einige Defizite bei ihrer Infrastruktur und den Fähigkeiten ihrer Mitarbeiter zu beseitigen. Tatsächlich besteht laut der Studie von Cisco der Hauptgrund für das Hosting von Netzwerken in der Cloud bei mittelständischen Unternehmen in der Überzeugung, die Cloud ermöglichte eine bessere Datensicherheit (68 Prozent). Am zweithäufigsten wurde als Grund genannt, dem Unternehmen fehlten genügend interne IT-Mitarbeiter (49 Prozent). (Siehe Abbildung 6.)

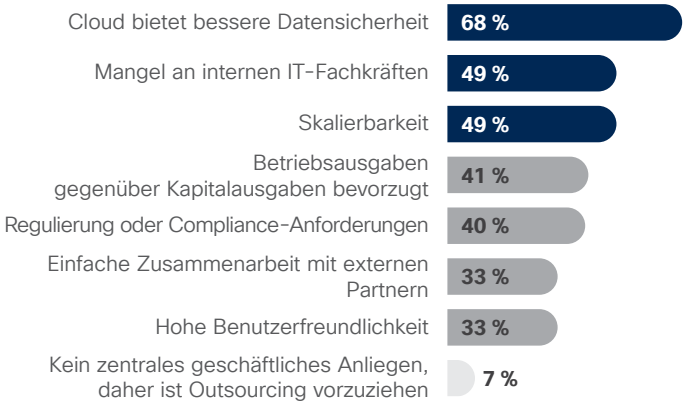
Darüber hinaus bevorzugen mittelständische Unternehmen die Cloud aufgrund ihrer Skalierbarkeit – also der geringeren Abhängigkeit des Unternehmens von seinen internen Ressourcen – und der flexiblen Umwandlung von Kapitalausgaben in Betriebsausgaben (Abbildung 6).

Abbildung 5: Mittelständische Unternehmen steigen verstärkt auf die Cloud um.



Quelle: Cisco Security Capabilities Benchmark Study 2018

Abbildung 6: Mittelständische Unternehmen wählen die Cloud für Sicherheit und Effizienz.



Quelle: Cisco Security Capabilities Benchmark Study 2018

Menschen: Die Suche nach Personal zur Stärkung der Sicherheit

Ein positives Ergebnis der Benchmark-Studie ist, dass in 92 Prozent der mittelständischen Unternehmen ein Mitglied der Geschäftsleitung für die Sicherheit verantwortlich ist. (Siehe Abbildung 7.)

Sofern sie über ausreichend Personal verfügen, sind mittelständische Unternehmen bereit, mehr Sicherheitstools wie erweiterten Endpunktschutz oder Web-App-Firewalls einzusetzen.

Eine Gemeinsamkeit zwischen Mittelstand und Großunternehmen besteht in einem Mangel an IT-Mitarbeitern, der die Fähigkeit zur Stärkung der Abwehrmechanismen behindert. Der Studie von Cisco zufolge sind schlicht nicht genügend interne Mitarbeiter für das Management von Tools zur Verbesserung der Sicherheit verfügbar.

Aus diesem Grund setzen viele kleine und mittelständische Unternehmen auf Outsourcing, um die Unterstützung zu erhalten, die sie zur Vertiefung ihrer Kenntnisse über Bedrohungen benötigen, um Kosten zu sparen und schneller auf Sicherheitsvorfälle reagieren zu können. Der Wunsch nach objektiven Einblicken wurde von mittelständischen Unternehmen am häufigsten als Begründung für das Outsourcing ihrer Sicherheitsaufgaben genannt (Abbildung 8), gefolgt von Kosteneffizienz und der Notwendigkeit einer umgehenden Reaktion auf Sicherheitsvorfälle.

Unterstützung durch Outsourcing ist eine gute Möglichkeit für Unternehmen, begrenzte Ressourcen optimal zu nutzen. Wenn sie aber davon ausgehen, ein Outsourcing-Anbieter oder Cloud-Partner könne alle Funktionen erfüllen, an denen es intern fehlt, können diese Unternehmen in Schwierigkeiten geraten.

Chad Paalman, CEO des Cisco Partners NuWave Technology Partners aus Kalamazoo im US-Bundesstaat Michigan, glaubt, in vielen kleinen und mittelständischen Unternehmen sei man sich nicht im Klaren darüber, in welchem Umfang die Outsourcing-Sicherheitsanbieter tatsächlich Analyse- und Überwachungsfunktionen leisteten.

Abbildung 7: Für die Sicherheit verantwortliche Mitglieder der Geschäftsleitung in mittelständischen Unternehmen

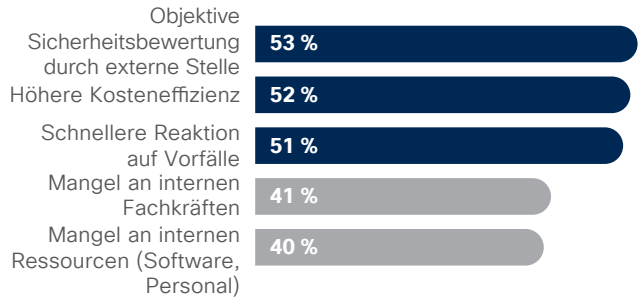
92 % haben ein für die Sicherheit verantwortliches Mitglied der Geschäftsleitung benannt

Titel des für die Sicherheit verantwortlichen Mitglieds der Geschäftsleitung

42 %	(CISO) Chief Information Security Officer
24 %	(CSO) Chief Security Officer
10 %	(CEO) Chief Executive Officer
8 %	(CIO) Chief Information Officer
3 %	(COO) Chief Operating Officer
5 %	(CTO) Chief Technology Officer
6 %	(SVP oder VP) Senior Vice President oder Vice President of IT
2 %	(CRO oder CCO) Chief Risk Officer oder Chief Compliance Officer

Quelle: Cisco Security Capabilities Benchmark Study 2018

Abbildung 8: Mittelständische Unternehmen nutzen Outsourcing, um den Mangel an internen Ressourcen auszugleichen.



Quelle: Cisco Security Capabilities Benchmark Study 2018

„Viele Führungskräfte kennen die Netzwerke ihrer Unternehmen nicht. Sie glauben, eine Firewall verhindere wie ein Türschloss alle unbefugten Zugriffe. Außerdem erwarten sie, wenn sie ihre Sicherheitsmaßnahmen einem Anbieter von Managed Services (MSP) übertragen, würden Protokolle überwacht, oder der Service würde auch Intrusion-Detection umfassen."

Chad Paalman, CEO von NuWave Technology Partners

Im Allgemeinen vertrauen kleine und mittelständische Unternehmen jedoch bei den folgenden Services auf ihre Outsourcing-Partner:

- Beratungsservices (57 Prozent)
- Incident-Response (54 Prozent)
- Sicherheitsüberwachung (51 Prozent)

Eher selten werden dagegen Aufgaben wie Threat-Intelligence an Outsourcing-Partner übertragen (39 Prozent). (Siehe Abbildung 9.)

Ein positiver Aspekt dabei ist, dass mittelständische Unternehmen offenbar einen Teil ihrer begrenzten Ressourcen für die Analyse von und die Reaktion auf Bedrohungen abstellen, um beispielsweise Threat-Intelligence und Incident-Response zu verbessern.

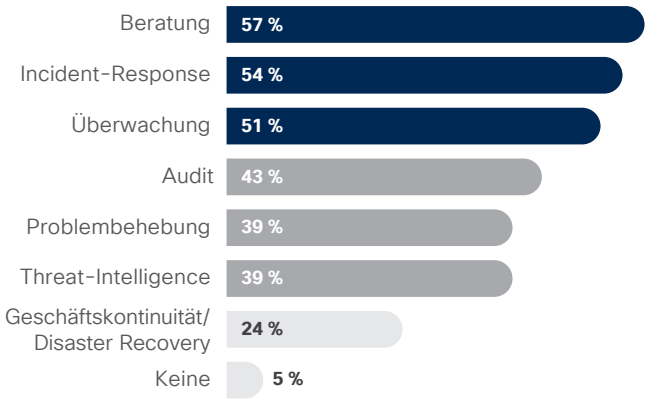
Prozesse: Regelmäßige Überprüfungen für das Sicherheitsmanagement

Umfassende, regelmäßige Sicherheitsprozesse – wie etwa Kontrollmechanismen für wertvolle Ressourcen und Überprüfungen der Sicherheitsmaßnahmen – helfen Unternehmen bei der Erkennung von Schwachstellen in ihren Verteidigungslinien. Solche Prozesse sind jedoch in kleinen und mittelständischen Unternehmen nicht so weit verbreitet, wie sie es sein sollten; möglicherweise aufgrund fehlenden Personals.

So werden laut der Cisco Security Capabilities Benchmark Study 2018 in mittelständischen Unternehmen seltener als in größeren Unternehmen Sicherheitsvorkehrungen regelmäßig überprüft, Sicherheitsfunktionen mithilfe von Tools unterstützt und Sicherheitsvorfälle routinemäßig untersucht (Abbildung 10).

Andererseits erklärten 91 Prozent der mittelständischen Unternehmen, sie hielten mindestens einmal jährlich Übungen ab, um ihre Incident-Response-Pläne zu testen. Wie auch bei der Abhängigkeit von Cloud- und Outsourcing-Partnern stellt sich jedoch auch hier die Frage, ob diese Incident-Response-Pläne ausreichen, um immer raffinierter vorgehende Angreifer abzuwehren.

Abbildung 9: Mittelständische Unternehmen übertragen Beratung und Incident-Response Outsourcing-Partnern.



Quelle: Cisco Security Capabilities Benchmark Study 2018

Abbildung 10: Mittelständische Unternehmen stimmen dem Einsatz betrieblicher Prozesse seltener uneingeschränkt zu.

Quelle: Cisco Security Capabilities Benchmark Study 2018

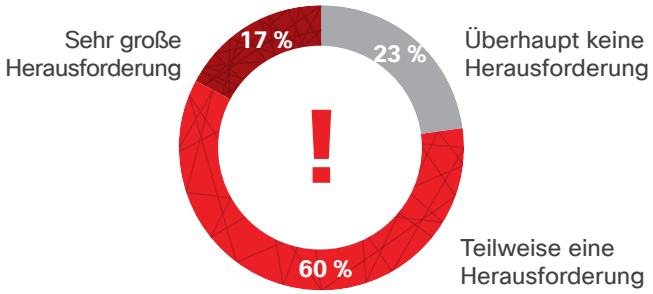
Vernetzung von Menschen, Prozessen und Technologie: Die Herausforderung der Orchestrierung

Wenn kleine und mittelständische Unternehmen ihre Verteidigungslinie um weitere Sicherheitsprodukte und Anbieter ergänzen – und IT-Ressourcen für das Management dieser Produkte umwidmen –, verbessern sie dadurch ihr Sicherheitsmanagement? Tatsächlich kann sogar das Gegenteil der Fall sein, zumindest in Bezug auf das Verständnis und die Orchestrierung von Sicherheitswarnungen.

Die meisten kleinen und mittelständischen Unternehmen erkennen heute, dass der Aufbau einer komplexeren Produkt- und Anbieterumgebung wachsende Verantwortlichkeiten mit sich bringt. So stufen 77 Prozent der mittelständischen Unternehmen die Orchestrierung der Warnungen verschiedener Lösungen als teilweise eine Herausforderung oder sogar als sehr große Herausforderung ein (Abbildung 11).

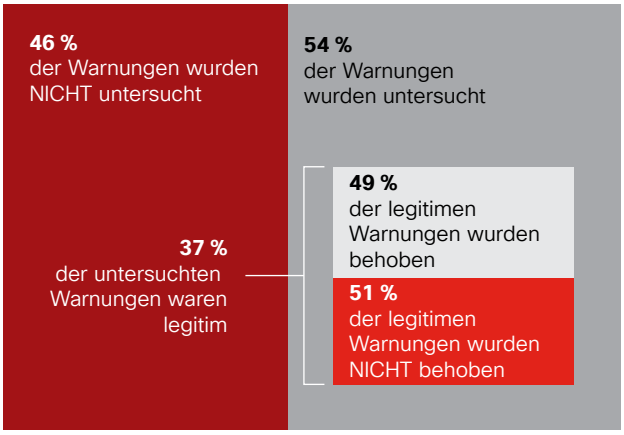
Beim Versuch einer Analyse dieser Warnungen können die Herausforderungen von Menschen, Prozessen und Technologie zusammen dazu führen, dass viele Warnungen nicht näher untersucht werden, wie in der Benchmark-Studie deutlich wurde (Abbildung 12).

Abbildung 11: Mittelständische Unternehmen stimmen dem Einsatz betrieblicher Prozesse seltener uneingeschränkt zu.



Quelle: Cisco Security Capabilities Benchmark Study 2018

Abbildung 12: Anteil der nicht untersuchten oder behobenen Sicherheitswarnungen



Quelle: Cisco Security Capabilities Benchmark Study 2018

Empfehlungen für die Zukunft

Technologie

Wenn Unternehmen den Einsatz neuer Tools erwägen, sollte im Idealfall die Anzahl der Anbieter und der Warnmeldungen, auf die reagiert werden muss, nicht weiter wachsen.

Stand bei der Entwicklung der Produkte also die Offenheit im Vordergrund? Wie lassen sie sich in Bezug auf die gemeinsame Nutzung von Daten und Threat-Intelligence in andere Produkte integrieren?
Gibt es eine Integrationsmöglichkeit für die Management-Konsole?

Wenn ein Anbieter behauptet, seine Produkte seien auf die Zusammenarbeit mit anderen ausgelegt, ist dies unmittelbar möglich, oder ist eine Programmierung per API durch den Käufer erforderlich?

Maschinelles Lernen ist trotz allen Hypes aus der modernen Sicherheit nicht mehr wegzudenken. Nutzen Sie maschinelles Lernen aber als zusätzliche Erkennungsebene bereits genutzter Produkte und nicht als eigenständiges Produkt eines anderen Anbieters, das nur zusätzlichen Managementaufwand verursachen würde.

Menschen und Prozesse

Im Klartext: Entwickeln Sie eine Strategie zur Verbesserung der Cybersicherheit. Nur 38 Prozent der kleinen und mittelständischen Unternehmen verfügen über eine aktive Strategie zur Bewältigung von Cyberrisiken, wie das Vistage Research Center, ein Ressourcen-Center für Führungskräfte, ermittelt hat.[6]

Berücksichtigt Ihre Planung angemessene Schulungen für die Endbenutzer? Decken Ihre Versicherungen Geschäftsverluste infolge eines Cyberangriffs ab? Gibt es Pläne zur Wahrung der Geschäftskontinuität und zur Kommunikation im Krisenfall, um eine schnellere Wiederherstellung zu ermöglichen und Rufschädigungen zu vermeiden?

Darüber hinaus müssen IT-Verantwortliche der Geschäftsleitung die wichtigsten Aspekte einer Sicherheitsverletzung deutlich erklären können:

- Wie sehen die Folgen für das Unternehmen aus?
- Welche Maßnahmen ergreift das Sicherheitsteam, um die Bedrohung einzudämmen und zu untersuchen? Wie lange dauert es bis zur Wiederaufnahme des Normalbetriebs?[7]

„Durch die Einführung einer Reihe von Sicherheitsplattformen und -tools, die miteinander zusammenarbeiten, anstelle verschiedener Teile, die möglicherweise sogar Konflikte verursachen, erreichen Sie neben höherer Sicherheitseffektivität auch eine Vereinfachung des Managements.“

**Ben M. Johnson,
CEO von Liberty Technology**

„Kleine und mittelständische Unternehmen sollten diese Risiken bewerten und Reaktionspläne entwickeln, bevor eine Sicherheitsverletzung stattfindet – nicht erst danach.“

**Chad Paalman,
NuWave Technology Partners**

6 Cyberthreats and Solutions for Small and Midsize Businesses, Vistage Research Center, 2018. Entwickelt in Zusammenarbeit mit Cisco und The National Center for the Middle Market. Verfügbar unter https://www.vistage.com/research-center/business-operations/risk-management/20180503-22912/.

7 Cisco Midyear Cybersecurity Report 2017: https://www.cisco.com/c/dam/global/es_mx/solutions/security/pdf/cisco-2017-midyear-cybersecurity-report.pdf. 13 Ebd.

Fazit

Eine letzte Empfehlung für kleine und mittelständische Unternehmen zur Förderung von Verbesserungen bei der Cybersicherheit: Sie sollten erkennen, dass schrittweise Änderungen besser sind als überhaupt keine Änderungen. Kurz gesagt: Statt gleich einen „perfekten“ Sicherheitsansatz anzustreben, sollten sie diesen zunächst „verbessern“. Perfektion ist – wie in allen anderen Belangen auch – unerreichbar.

Kleine und mittelständische Unternehmen müssen zudem verstehen, dass es keine „universelle“ Technologielösung zur Bewältigung sämtlicher Herausforderungen bei der Cybersicherheit gibt. Dafür ist die Bedrohungslandschaft schlicht zu komplex und zu dynamisch. Die Angriffsfläche wird immer größer und verändert sich ständig. Als Reaktion darauf müssen auch Sicherheitstechnologien und -strategien kontinuierlich weiterentwickelt werden.

Weitere Informationen zum bedrohungsorientierten Sicherheitsansatz von Cisco finden Sie unter cisco.com/go/security.

Hauptgeschäftsstelle Nord- und Südamerika
Cisco Systems, Inc.
San Jose, CA

Hauptgeschäftsstelle Asien-Pazifik-Raum
Cisco Systems (USA) Pte. Ltd.
Singapur

Hauptgeschäftsstelle Europa
Cisco Systems International BV Amsterdam,
Niederlande

Cisco verfügt über mehr als 200 Niederlassungen weltweit. Die Adressen mit Telefon- und Faxnummern finden Sie auf der Cisco Website unter www.cisco.com/go/offices.

Veröffentlicht im Juli 2018