



STUDIE SECURITY AUTOMATION 2017

GOLD-PARTNER



SILBER-PARTNER





Ein aktuelles Studienprojekt von



Gold-Partner



Silber-Partner



Alle Angaben in diesem Ergebnisband wurden mit größter Sorgfalt zusammengestellt. Trotzdem sind Fehler nicht ausgeschlossen. Verlag, Redaktion und Herausgeber weisen darauf hin, dass sie weder eine Garantie noch eine juristische Verantwortung oder jegliche Haftung für Folgen, die auf fehlerhafte Informationen zurückzuführen sind, übernehmen.

Der vorliegende Ergebnisberichtsband, einschließlich all seiner Teile, ist urheberrechtlich geschützt. Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen, auch auszugsweise, bedürfen der schriftlichen Genehmigung durch IDG Research Services.



Sicherheit automatisieren? Geht das überhaupt?

Jedenfalls sehen immer mehr Technologieentscheider die Notwendigkeit, durch automatisierte Prozesse die Anfälligkeit ihrer Organisation für zunehmend asymmetrische Bedrohungsszenarien zu verringern. Die Automatisierung verspricht dabei vor allem Geschwindigkeit. Und darauf kommt es mehr denn je an. Im Cyber-Raum werden die Angriffe immer versierter und bedürfen intelligenterer Systeme, die in der Lage sind, ad hoc, im besten Fall prädiktiv, aber in jedem Fall analytisch zu (re-)agieren. Hier schließt sich der Kreis zwischen automatisierter Sicherheit und Künstlicher Intelligenz.



Michael Beilfuß
Verlagsleiter

Naturgemäß werden die Chancen, die in Security Automation stecken, in einer noch frühen Phase der Marktentwicklung vor allem von größeren Unternehmen erkannt. Diese verfügen über komplexere IT-Landschaften und sind daher einer noch größeren Vielfalt von Bedrohungen ausgesetzt. Die Ressourcenlage kann mit dem steigenden Risiko natürlich nicht Schritt halten. Hier liegt das große Potenzial von Security-Automation-Lösungen – beginnend mit der automatisierten Konfiguration der Firewall über das Patch-Management bis hin zu schon ambitionierten Einsatzfeldern wie dem Thread Monitoring.

Bereits die Hälfte der befragten Manager nutzen Managed-Security-Services. Das Bewusstsein für den technologischen und erfahrungsmäßigen Vorsprung, der durch Managed-Services auch im hochsensiblen Sicherheitsumfeld gewonnen werden kann, ist also schon breitflächig vorhanden. Eine gute Nachricht. Noch besser: Security Automation zeigt sich in der vorliegenden Studie als herausragendes Wachstumsfeld für Managed-Services der nächsten Generation. Aber es gibt auch ganz zentrale Aufgaben, die noch ungelöst sind: Das deutlich geringere Bewusstsein, der punktuell fehlende Fokus, die möglicherweise mangelnde Ressourcenausstattung in weiten Teilen der kleineren und mittelgroßen Unternehmen sind besorgniserregend. In einer maximal vernetzten Ökonomie, in der kein Unternehmensnetzwerk, kein einzelnes Device mehr als „technologische Insel“ existiert, ist die Verbesserung der Sicherheitsstandards gerade im KMU-Bereich eine wichtige Aufgabe.

Wir wünschen Ihnen eine erkenntnisreiche Lektüre!

Michael Beilfuß

Inhalt



Editorial

3



Management Summary

Die Key Findings im Überblick	6
Die Key Findings im Einzelnen	
1. Cyber-Angriffe werden immer gefährlicher	9
2. Security Automation ist nur bedingt im Fokus	10
3. Security Automation gewinnt an Bedeutung	11
4. Klares Votum für automatisierte Sicherheitslösungen.....	12
5. Schnelle Reaktion punktet	13
6. Investitionsbereitschaft noch ausbaufähig.....	14
7. Optimierungsbedarf: Mangelnde Automatisierung ist ein Problem.....	15
8. Automatisierung: Firewalls und Patch-Management dominieren	16
9. Bei Security Automation kommen externe Dienstleister zum Zuge.....	18
10. Backup sowie Zugangs- und Rechtekontrolle sind beliebteste Schutzvorkehrungen.....	20

6



Studiendesign

Studiensteckbrief.....	37
Stichprobenstatistik.....	38

36



Weitere Studienergebnisse

1. Cyber-Angriffe sind eine konkrete Gefahr.....	22
2. Vielfältige Bedrohungsszenarien.....	23
3. Sicherheitsstrategie: IT-Sicherheitslösungen haben Vorrang.....	24
4. IT-Security-Risiken: Schadsoftware auf Platz eins.....	25
5. Unternehmen geben sich gute Noten bezüglich ihres IT-Security-Niveaus.....	26
6. IT-Leiter und CIOs entscheiden.....	27
7. Kooperation mit IT-Sicherheitsdienstleistern auf vielen Gebieten.....	28
8. Der Preis allein entscheidet nicht.....	29
9. Hohe Zufriedenheit mit Dienstleistern im Bereich IT-Sicherheit..	30
10. IT-Sicherheitsstrategie vor Cloud und Digitalisierung.....	32
11. Den Ernstfall übt nur die Hälfte der Unternehmen.....	33

21



Unsere Gold-Studienpartner stellen sich vor

FireEye Deutschland GmbH.....	40
NTT Security.....	42

39



Blick in die Zukunft

Gut angelaufen – viel bleibt zu tun

34



Studienreihe

44

Die Key Findings im Einzelnen





1. Cyber-Angriffe werden immer gefährlicher

Die größten Herausforderungen für Unternehmen: die wachsende Komplexität von Cyber-Attacken und die Notwendigkeit, schnellstmöglich auf solche Bedrohungen zu reagieren.

Knapp drei Viertel der Unternehmen sehen in immer versierteren Angriffen auf IT-Systeme die größte Herausforderung im Bereich IT-Sicherheit.

Cyber-Attacken müssen umgehend gestoppt werden. Die zeitnahe Reaktion auf neue Sicherheitsbedrohungen stellt jedoch 55 Prozent der Befragten vor Probleme. Dies gilt für Unternehmen jeder Größe, unabhängig vom Budget für IT-Sicherheitsmaßnahmen.

Rund 36 Prozent der Studienteilnehmer betrachten das mangelnde Sicherheitsbewusstsein der eigenen Mitarbeiter als Herausforderung. Vor allem für kleinere Unternehmen mit bis zu 100 Mitarbeitern ist das ein Problem (40 Prozent), dagegen nur für 25 Prozent der Firmen mit mehr als 1.000 Beschäftigten.

Die Kontrolle über Daten und Anwendungen in der Cloud sowie die wachsende Komplexität von IT-Infrastrukturen, etwa durch Hybrid Cloud, sind nur für jeweils rund ein Viertel der Befragten große Herausforderungen im Bereich IT-Security.

Was sind in Ihren Augen für die Unternehmen die großen Herausforderungen in Bezug auf IT-Security?

Mehrfachantworten möglich. Angaben in Prozent. Dargestellt sind Nennungen mit über 20 Prozent. Basis: n = 408

Die wachsende Bedrohung durch immer komplexere Cyber-Angriffe	73,5
Die zeitnahe Reaktion auf neue Sicherheitsbedrohungen	55,4
Implementierung von Sicherheitsstandards im Unternehmen	40,7
Der Aufwand für die kontinuierliche Überwachung der Einhaltung von Sicherheitsvorgaben	37,3
Fehlende Security-Awareness/fehlendes Training bei eigenen Mitarbeitern	36,5
Das Risikopotenzial, das von internen Mitarbeitern ausgeht	35,5
Priorisierung von IT-Security auf Vorstands- und Managementebene	32,1
Echtzeitüberblick über alle Aktivitäten in Systemen, Netzwerken, Datenbanken & Anwendungen	30,6
Zu wenige IT-Fachkräfte im Unternehmen (Anzahl der Mitarbeiterstellen)	29,9
Zu niedriges IT-Security-Budget	29,7
Die wachsende Komplexität von IT-Infrastrukturen, etwa durch Hybrid Clouds	25,7
Die abnehmende Kontrolle über Daten und Anwendungen durch Cloud Computing	23,3
Die Schulung von End-Usern in Bezug auf IT-Sicherheit	22,5
Fachkräftemangel im Markt	20,6
Fehlende Informationen über den Wert von bedrohten Daten und Prozessen	20,1
Die Absicherung von Daten, die in einer Cloud gespeichert und bearbeitet werden	20,1

Weitere Studienergebnisse



1. Cyber-Angriffe sind eine konkrete Gefahr

Die Mehrzahl der Unternehmen wurde in den vergangenen 24 Monaten mindestens einmal Ziel einer Attacke durch externe oder interne Hacker.

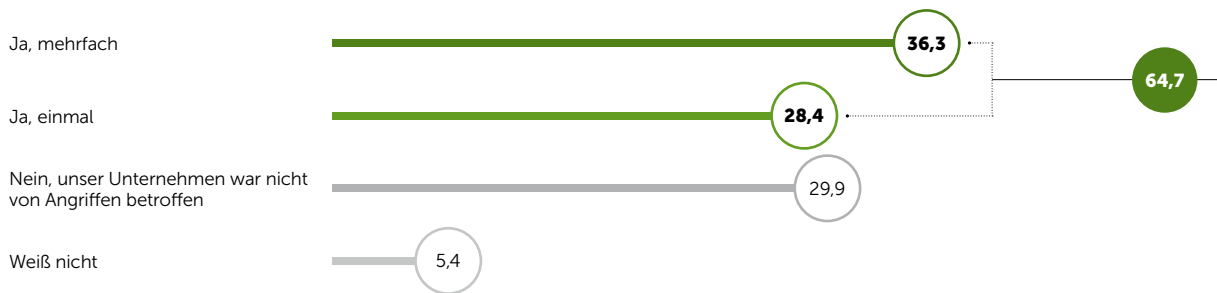
Fast zwei Drittel der befragten Unternehmen verzeichneten in den beiden vergangenen Jahren mindestens einen Cyber-Angriff. 36 Prozent sprechen sogar von mehrfachen Angriffen.

Von den großen Unternehmen waren rund drei Viertel Ziel eines oder mehrerer Angriffe, etwas geringer ist der Anteil der kleinen und mittelgroßen Unternehmen (57 und 64 Prozent).

Bei 65 Prozent der betroffenen Unternehmen führten Cyber-Angriffe zu Störungen von Arbeitsprozessen. In 22 Prozent der Fälle kam es sogar zu massiven Beeinträchtigungen.

War Ihr Unternehmen in den vergangenen beiden Jahren Ziel von Angriffen?

Angaben in Prozent. Basis: n = 408



Ergebnis-Split nach Anzahl der Mitarbeiter

	unter 100	100 – 999	1.000 +
Ja, mehrfach	27,8	32,1	48,9
Ja, einmal	29,6	31,5	23,7
Nein, unser Unternehmen war nicht von Angriffen betroffen	37,4	30,9	22,1
Weiß nicht	5,2	5,6	5,3

Haben IT-Sicherheitsprobleme aufgrund der Angriffe zu Störungen der Arbeitsprozesse geführt?

Angaben in Prozent. Basis: n = 263. Filter: nur die Befragten, die bereits von Angriffen betroffen waren.

