COMPUTERWOCHE CIO ChannelPartner TECCHANNEL IT IM MITTELSTAND

IDG RESEARCH SERVICES

STUDIE SECURITY AUTOMATION 2017

GOLD-PARTNER

FireEye NTT Security

SILBER-PARTNER

baramundi HORNETSECURITY®

Ein aktuelles Studienprojekt von

IDG
RESEARCH SERVICES

Gold-Partner

FireEye NTT Security

Silber-Partner

baramundi HORNETSECURITY®

Sicherheit automatisieren? Geht das überhaupt?

Michael Beilfuß
Verlagsleiter

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.

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

Weitere Studienergebnisse

21

Unsere Gold-Studienpartner stellen sich vor

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.

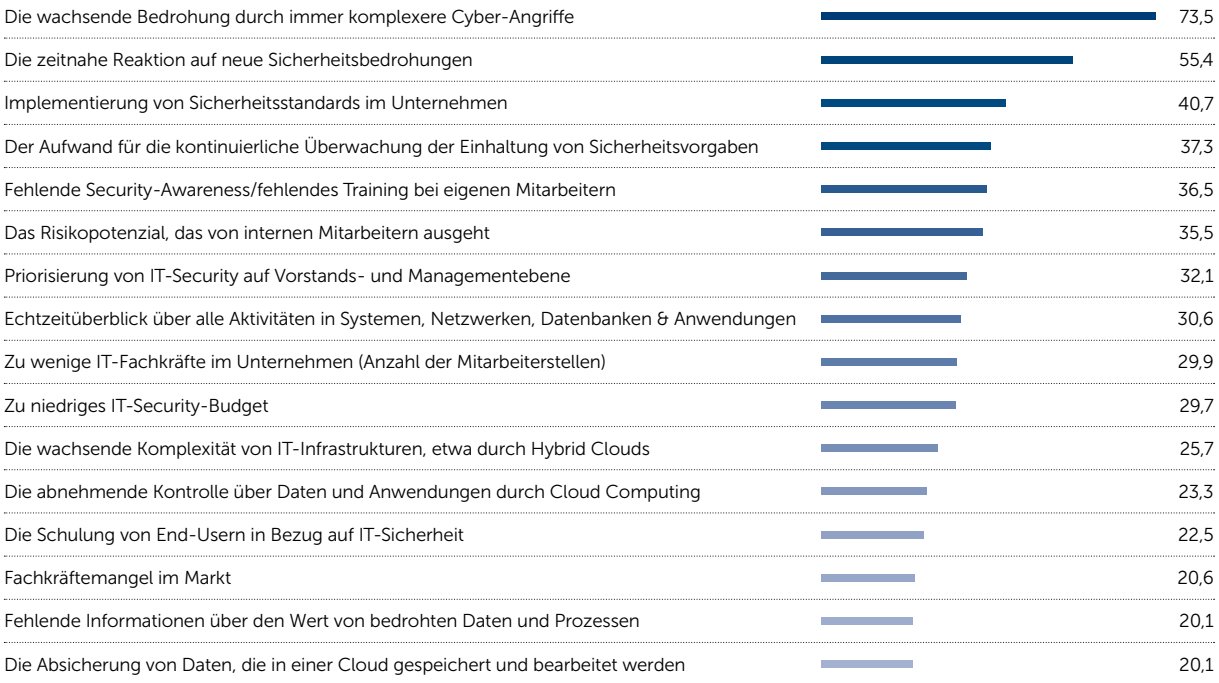
Cyber-Attacken müssen umgehend gestoppt werden. Die zeitnahe Reaktion auf neue Sicherheitsbedrohungen stellt jedoch 55 Prozent der Befragten vor Probleme. Dies gilt für Unternehmen jeder Größe, unabhängig vom Budget für IT-Sicherheitsmaßnahmen.

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 Beschäftigen.

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



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.

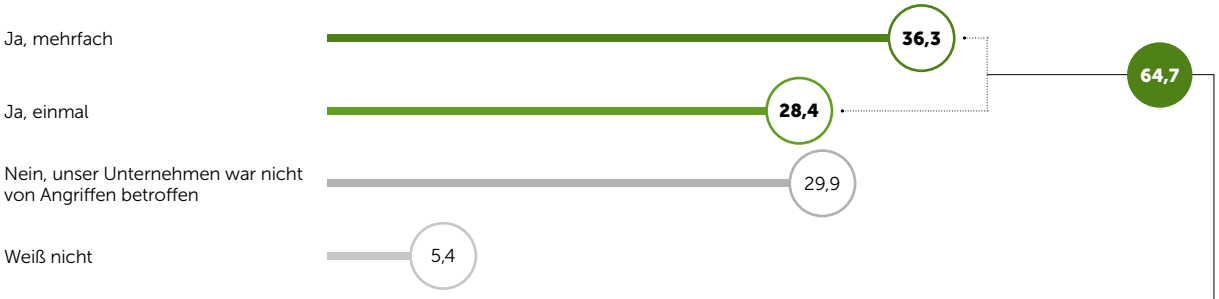
Fast zwei Drittel der befragten Unternehmen verzeichneten in den beiden vergangenen Jahren mindestens einen Cyber-Angriff. 36 Prozent sprechen sogar von mehrfachen Angriffen.

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.