



Gigamon®

2018 CYBERTHREAT DEFENSE REPORT

Der fünfte jährliche Cyberthreat Defense Report der CyberEdge Group enthüllt, wie IT-Sicherheitsexperten die Sicherheitssituation ihrer Unternehmen, die Herausforderungen beim Schaffen effektiver Schutzmaßnahmen gegen Cyberbedrohungen und die Pläne für die Bewältigung dieser Herausforderungen einschätzen. Im Folgenden finden Sie einige der wichtigsten Ergebnisse des diesjährigen Berichts.

DATENPANNEN SIND UNUMGÄNGLICH

Unternehmen fallen immer öfter erfolgreichen Cyberangriffen zum Opfer ...
Besserung ist nicht in Sicht.



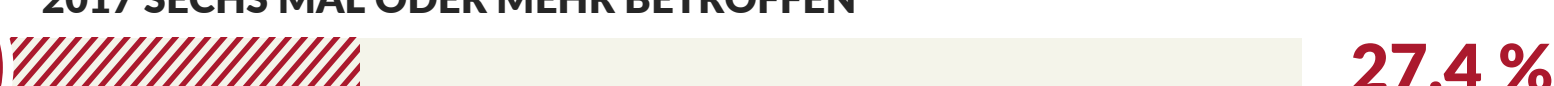
2017 MINDESTENS EINMAL BETROFFEN



77,2 %



2017 SECHS MAL ODER MEHR BETROFFEN



27,4 %



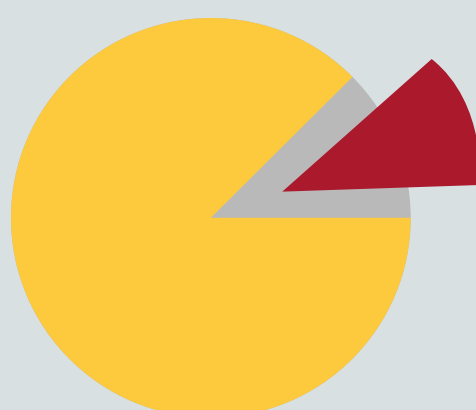
ERWARTEN, 2018 BETROFFEN ZU SEIN



62,3 %

SICHERHEITSBUDGETS STEIGEN

Als Reaktion darauf haben Unternehmen die Ausgaben für Sicherheitsprodukte, -dienstleistungen und -personal 2018 um etwa 4,7 % erhöht.



12 %

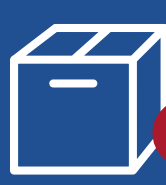
Beträgt der durchschnittliche Anteil von IT-Budgets, der für Sicherheit ausgegeben wird

ABER DIE GEFAHR IST NOCH IMMER NICHT GEBANNT

HERAUSFORDERUNG NR. 1: ZU VIEL ZU TUN

Je größer der technologische Fußabdruck der modernen Unternehmen, desto größer die zu verteidigende Angriffsfläche.

INFRASTRUKTUR MIT DER NIEDRIGSTEN SICHERHEITSBEWERTUNG



Container



Mobilgeräte



Cloud-Infrastruktur

PROZESSE/FUNKTIONEN MIT DEN GRÖßTEN MÄNGELN



Entwickeln und Testen von Anwendungen (SDLC)



Angriffsflächen-reduzierung



Erkennung von verdächtigen Insidern/ Insiderangriffen

EINE GROßE HÜRDE HINSICHTLICH EFFEKTIVITÄT



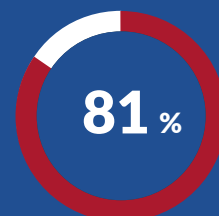
Zu viele Daten für eine Analyse

HERAUSFORDERUNG NR. 2: MANGEL AN FACHPERSONAL

Es ist nur ein kleiner Trost, mehr Geld für Sicherheit zur Verfügung zu haben, wenn ein weltweiter Mangel an Cybersicherheitsexperten besteht.



Der Mangel an Fachpersonal wurde als größtes Hindernis für den angemessenen Schutz vor Cyberbedrohungen eingestuft.



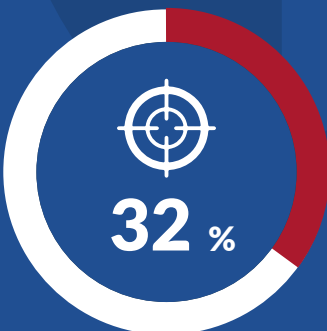
Anteil der Unternehmen, die unter dem Mangel an IT-Fachkräften leiden

Bildung	87 %
Technologie	85 %
Fertigung	82 %
Finanzen	81 %

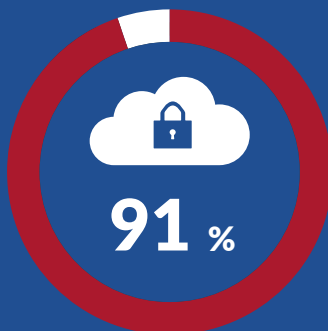
Vom IT-Fachkräftemangel betroffene Branchen

HERAUSFORDERUNG NR. 3: DIE RICHTIGEN LÖSUNGEN SIND SCHWER ZU FINDEN

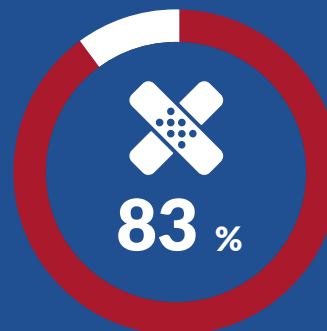
Viele Unternehmen schaffen es bisher nicht, angemessen und an den richtigen Stellen in Technologie zu investieren und dabei den größtmöglichen Wert aus den Investitionen zu ziehen.



Weniger als ein Drittel aller Unternehmen haben ausreichend in die Erkennung von Cyberbedrohungen investiert.



Mehr als neun von zehn Unternehmen sehen sich großen Herausforderungen in Sachen Cloud-Sicherheit gegenüber.



Mehr als vier von fünf Unternehmen haben Schwierigkeiten dabei, bekannte Schwachstellen zeitnah zu beheben.

EINEN KURS FÜR DIE ZUKUNFT FESTLEGEN

Um die Herausforderungen moderner Unternehmen hinsichtlich der IT-Sicherheit zu bewältigen, braucht es Cyberschutzmaßnahmen, die „einfach funktionieren“, z. B. indem sie:



Umfassende Sichtbarkeit bieten



Sicherheitsinfrastruktur auslagern und vereinfachen



Die Bereitstellung und Integration neuer Sicherheitstools beschleunigen



Orchestrierung und Automatisierung ermöglichen