KEIN DIGITALER WANDEL OHNE
ZERO TRUST
SICHERHEITSMODELL

DER DIGITALE WANDEL ERFORDERT EINE WEITERENTWICKLUNG DER UNTERNEHMENSSICHERHEIT UND -NETZWERKE.

NUTZER, GERÄTE, ANWENDUNGEN UND DATEN BEFINDEN SICH ZUNEHMEND AUSSERHALB DES KLASSISCHEN NETZWERKRANDS. DAMIT ENTZIEHEN SIE SICH EINER UMFASSENDEN KONTROLLE.

40 %

Bei **40,8 %** der Unternehmen arbeiten 21–40 % der Mitarbeiter extern. Bei **25,7 %** arbeiten über 40 % der Mitarbeiter extern.[1]

67 %

Mehr als **67 %** der Arbeitnehmer nutzen bei der Arbeit eigene Geräte.[2]

80 %

80 % aller BYOD-Geräte sind vollständig ungemanagt.[3]

50 %

Unternehmen nutzen fast während **50 %** der Zeit cloudbasierte Anwendungen.[4]

10 %

Weniger als **10 %** aller Unternehmen geben an, genau zu wissen, welche Geräte auf ihr Netzwerk zugreifen.[5]

DER DIGITALE WANDEL SCHAFFT NEUE GESCHÄFTSPROZESSE, DIE DIE ANGRIFFSFLÄCHE VERGRÖSSERN.

63 %

der Datenschutzverletzungen wurden durch Drittanbieter verursacht.[6]

390.000

neue Schadprogramme werden täglich registriert.[7]

1/3

der Mobilgeräte weisen ein mittleres bis hohes Risiko für Datenverlust auf.[8]

40.000.000

Die Anzahl der in beliebten Mobilgeräten gefundenen schädlichen Installationspakete hat sich 2016 verdreifacht: auf ca. **40 Millionen** Angriffe.[9]

3,5 x

Das Volumen mobiler Ransomware stieg in den ersten Monaten 2017 um das **3,5-Fache**.[10]

„VERTRAUEN UND KONTROLLE" IST NICHT LÄNGER EINE OPTION, DENN DIE BEDROHUNGEN BEFINDEN SICH INNERHALB DES NETZWERKRANDS.

› 40 %

der Verstöße entstehen durch autorisierte Nutzer, die jedoch auf nicht autorisierte Systeme zugreifen.[11]

70 %

der Unternehmen erlebten im vergangenen Jahr einen Sicherheitsvorfall, der sich negativ auf ihr Geschäft ausgewirkt hat.[12]

3 x

Die Anzahl der Ransomware-Angriffe auf Unternehmen hat sich im letzten Jahr verdreifacht: Während entsprechende Angriffe im ersten Quartal noch alle zwei Minuten erfolgten, betrug der Abstand im dritten Quartal nur noch 40 Sekunden.[13]

4,3 x

Es gab 4,3 Mal mehr neue Ransomware-Varianten im 1. Quartal 2017 als im 1. Quartal 2016.[14]

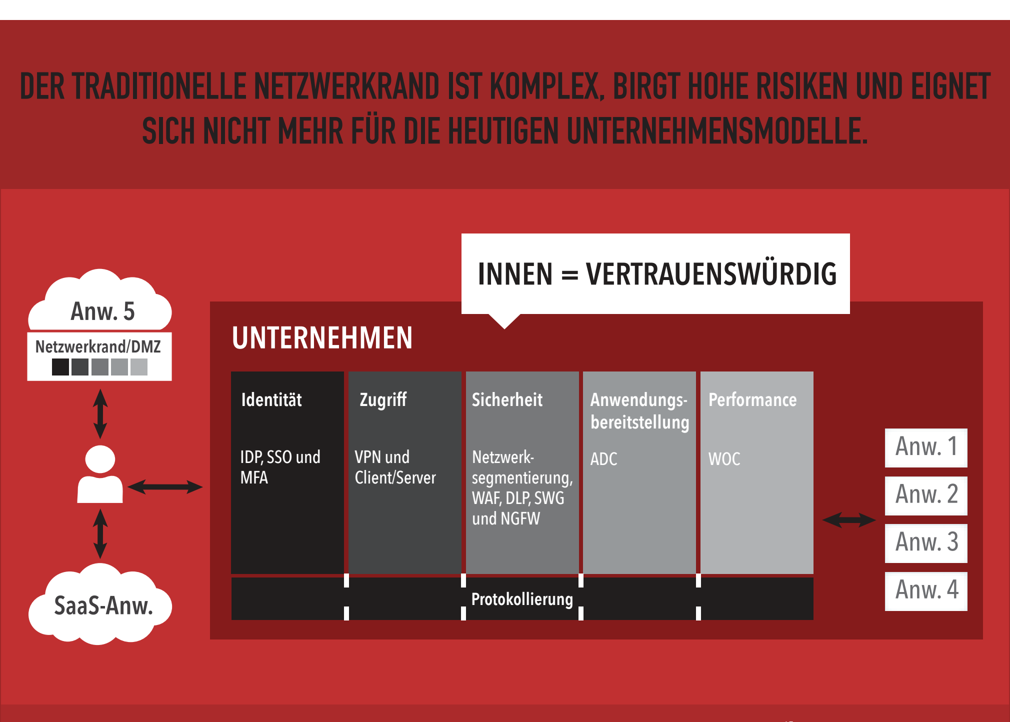
‹ 19 %

Weniger als 19 % der Datenschutzvorfälle wurden selbst erkannt.[15]

› 90 %

Mehr als 90 % der Malware nutzt das DNS, um sich im Unternehmen zu bewegen.[16]

DER TRADITIONELLE NETZWERKRAND IST KOMPLEX, BIRGT HOHE RISIKEN UND EIGNET SICH NICHT MEHR FÜR DIE HEUTIGEN UNTERNEHMENSMODELLE.



75 % der Unternehmen nutzen bis zu 14 Netzwerk- und Anwendungskomponenten.[17]

ERWARTUNG

INNEN = VERTRAUENSWÜRDIG

IM VGL. ZU

REALITÄT

ES GIBT KEIN INNEN …

- Nutzer und Anwendungen im Netzwerkrand
- Vertrauen und Kontrolle
- Vollständiger Netzwerkzugriff

- Nutzer und Anwendungen überall
- Kontrolle und KEIN Vertrauen
- Zugriff auf Anwendungsebene

41 % der IT-Experten bewerten Komplexität als größtes Problem von Architekturen/Integrationen.[18]

IM UNTERNEHMENSNETZWERK WERDEN IMMER MEHR UNTERSCHIEDLICHE GERÄTE VERWENDET. DIE GRENZE ZWISCHEN INNEN UND AUSSEN VERSCHWIMMT ZUSEHENDS.

20,4 MILLIARDEN

Gartner schätzt, dass bis 2020 mehr als **20,4 Milliarden** IoT-Geräte installiert sein werden.[19]

80 %

der IoT-Anwendungen bzw. 71 % der Apps werden nicht auf Schwachstellen getestet.[20]

90 %

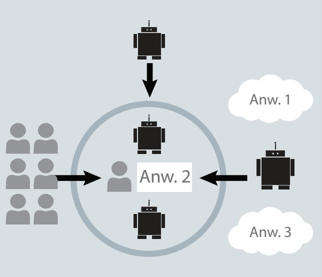
der Menschen haben ein Mobilgerät in Reichweite.[21]

Sollten Sie diesem Gerät in Ihrem Netzwerk vertrauen? Sehen Sie, was in einer Woche alles passieren kann.

ZEIT FÜR EINEN CLOUDNETZWERKRAND

Mit einem Zero-Trust-Modell für Sicherheit und Bereitstellung meistern Sie den digitalen Wandel – und sichern Ihre Netzwerke.

- Unterscheiden Sie nicht zwischen Innen und Außen.
- Alles ist „Außen", ganz wie im Internet.



- Überprüfen Sie alles – vertrauen Sie niemandem.
- Stellen Sie Anwendungen und Daten nur authentifizierten und autorisierten Nutzern und Geräten bereit.

ZERO TRUST

- Überprüfen Sie Nutzer immer durch Protokollierung und Verhaltensanalyse.
- Transparenz ist essenziell: Wir müssen wissen, was „normal" ist.

WELCHE UNTERSTÜTZUNG KANN AKAMAI HIER BIETEN?

Akamai hat die weltweit sicherste, zuverlässigste, skalierbarste und leistungsstärkste Plattform entwickelt. Damit können Sie sich bei der Nutzung dieses gefährlichen und risikoreichen Ökosystems beruhigt zurücklehnen. Weitere Informationen finden Sie unter akamai.com/zerotrust.

QUELLEN

1. IDC InfoBrief, gesponsert von Akamai, Remotezugriff und Sicherheit, September 2017
2. CBS Money
https://www.cbsnews.com/news/byod-alert-confidential-data-on-personal-devices
3. https://www.securedgenetworks.com/blog/topic/strategy
4. https://www.forbes.com/forbes/welcome/?toURL=https://www.forbes.com/sites/louiscolumbus/2017/05/14/enterprises-are-running-cloud-based-apps-nearly-50-of-the-time/
5. https://www.securedgenetworks.com/blog/topic/strategy
6. IDC InfoBrief, gesponsert von Akamai, Remotezugriff und Sicherheit, September 2017
7. https://www.av-test.org/de/statistiken/malware
8. https://www.skycure.com/wp-content/uploads/2016/06/Skycure-Q1-2016-MobileThreatIntelligenceReport.pdf
9. Kaspersky-Bericht zur Entwicklung mobiler Malware 2016
10. Malware-Bericht für das 1. Quartal 2017 von Kaspersky Lab
11. IDC InfoBrief, gesponsert von Akamai, Remotezugriff und Sicherheit, September 2017
12. Cybersecurity Poverty Index 2016 von RSA
https://www.rsa.com/de-de/resources/rsa-cybersecurity-poverty-index-2016
13. https://securelist.com/kaspersky-security-bulletin-2016-story-of-the-year/76757
14. https://blog.barkly.com/ransomware-statistics-2017
15. Infocyte: Lücken bei der Vorfallserkennung und Strategien, um sie zu schließen
https://www.infocyte.com/breach-detection-gap-conf
16. Cisco Annual Security Report 2016
17. IDC InfoBrief, gesponsert von Akamai, Remotezugriff und Sicherheit, September 2017
18. IDC InfoBrief, gesponsert von Akamai, Remotezugriff und Sicherheit, September 2017
19. http://www.gartner.com/newsroom/id/3598917
20. Arxan: Studie zur Sicherheit von Apps und IoT-Anwendungen 2017
https://www.arxan.com/2017-Ponemon-Mobile-Iot-Study
21. Pew-Forschungszentrum in Huffington Post
https://track.akamai.com/Pew%20Research%20Center

Akamai

Als weltweit größte und renommierteste Plattform für die Cloudbereitstellung unterstützt Akamai seine Kunden dabei, ein optimales und sicheres digitales Erlebnis bereitzustellen – auf jedem Gerät, an jedem Ort und zu jeder Zeit. Die stark verteilte Plattform von Akamai weist mit über 200.000 Servern in 130 Ländern eine beispiellose Skalierbarkeit auf und bietet Kunden somit eine überragende Performance sowie einen umfassenden Bedrohungsschutz. Das Akamai-Portfolio für Website- und App-Performance, Cloudsicherheit sowie Unternehmenszugriff und Videobereitstellung wird durch einen herausragenden Kundenservice und Rund-um-die-Uhr-Überwachung begleitet. Warum führende Finanzinstitute, E-Commerce-Unternehmen, Medien- und Unterhaltungsanbieter sowie Behörden auf Akamai vertrauen, erfahren Sie unter www.akamai.de, im Blog blogs.akamai.com/de oder auf Twitter unter @AkamaiDACH oder @Akamai. Unsere globalen Standorte finden Sie unter www.akamai.de/locations.

Veröffentlicht: Oktober 2017