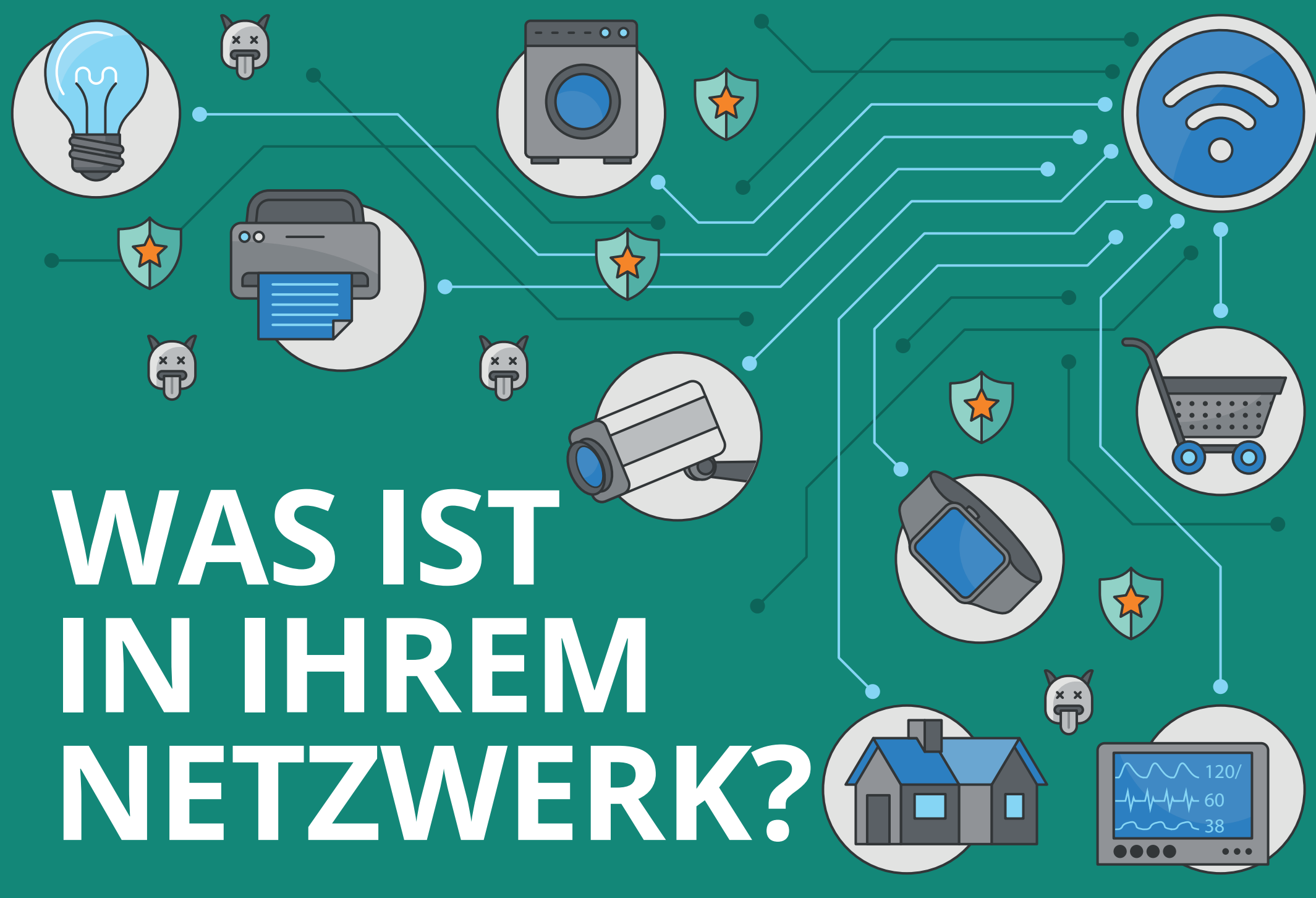




WAS IST IN IHREM NETZWERK?

Das Internet of Things (IoT), immer erreichbare mobile Mitarbeiter und das BYOD-Konzept sind Beispiele für Entwicklungen, durch die die IT-Infrastrukturen in den Unternehmen immer komplexer und dadurch wesentlich anfälliger als bisher für Cyberattacken werden.

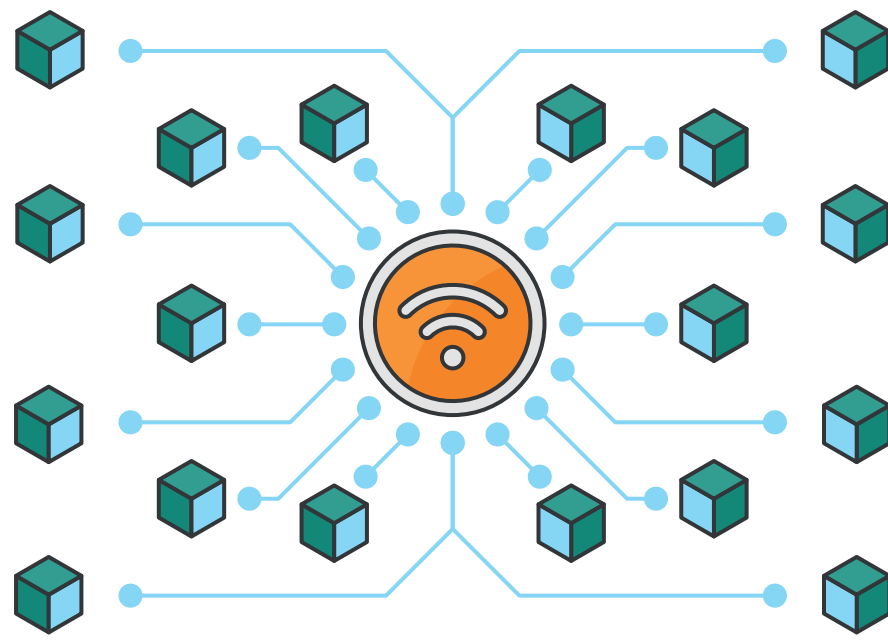
Ist Ihr Unternehmen darauf vorbereitet?

IoT: Eine Realität ... die weiter wächst!

Das IoT verbreitet sich mit enormer Geschwindigkeit, sodass es Unternehmen zunehmend schwer fällt, für eine effiziente Verwaltung und Sicherheit zu sorgen.

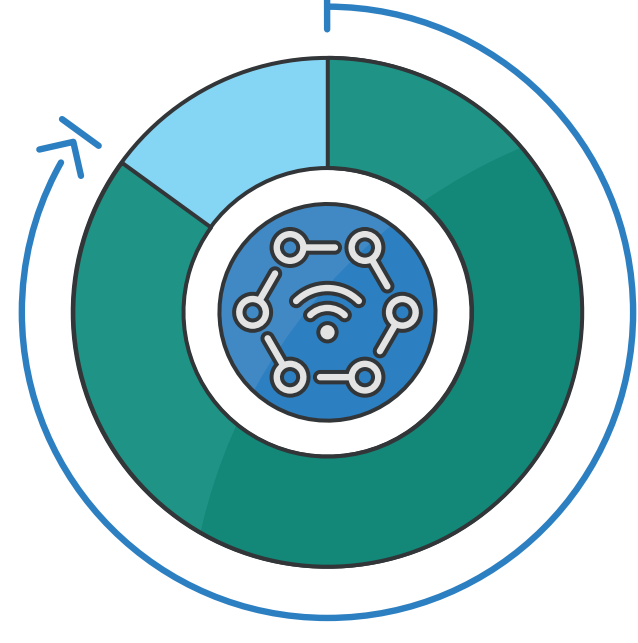
8,4 Mrd. „Dinge“

werden Schätzungen nach bis 2017 mit Netzwerken verbunden sein.¹



85 % der Unternehmen

werden bis 2019 das IoT in ihren Netzwerken implementieren.²



Wie sichern Sie Ihr Unternehmen und Ihre Infrastruktur gegen das IoT? CIOs und CISOs kennen mittlerweile die Fakten:

8 von 10 Unternehmen

hatten es bereits mit einer IoT-spezifischen Sicherheitsverletzung zu tun.³



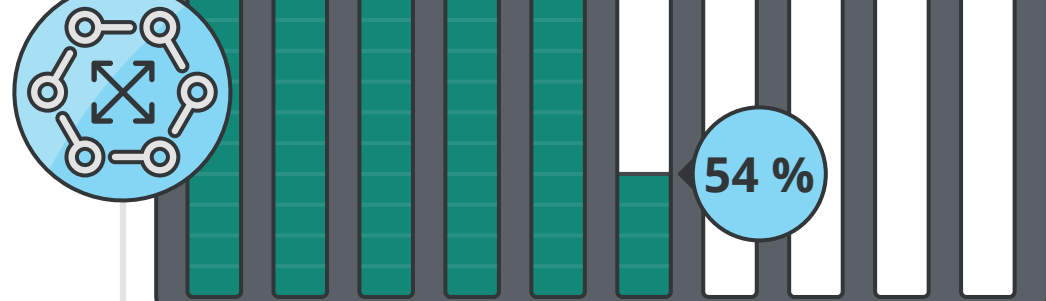
IoT-Sicherheit – ein Thema in den IT-Abteilungen

Die IT-Abteilungen stehen unter Druck. Die Unternehmensverantwortlichen fordern mehr Anwendungen und Geräte und die Einbindung von mehr „Dingen“, die überwachen können und überwacht werden müssen. Für alles muss es eine eigene App geben – und zwar im gesamten Unternehmensnetzwerk. Das Ergebnis: Sicherheitsrisiko **steigen**, Transparenz und Produktivität **sinken**.

Laut einer ESG-Studie bestätigen selbst die Befürworter von mehr Cybersicherheit die Mehrbelastung durch das IoT⁴:

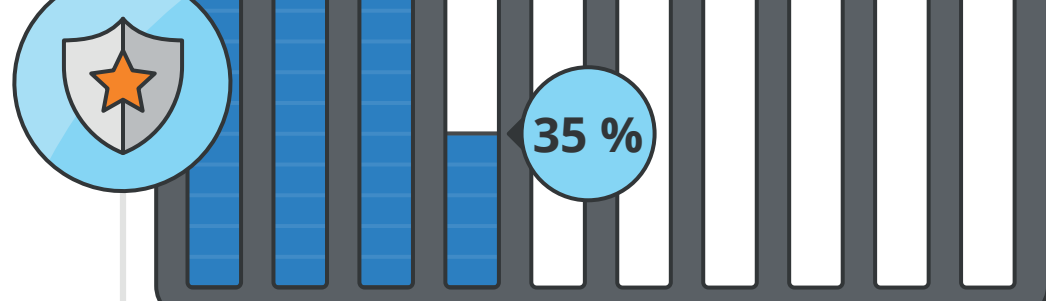
54 %

Die meisten Befragten geben an, dass das fehlende Know-how bei der Cybersicherheit zu mehr Arbeitsbelastungen und zu einer Überlastung der Analysten geführt hat.



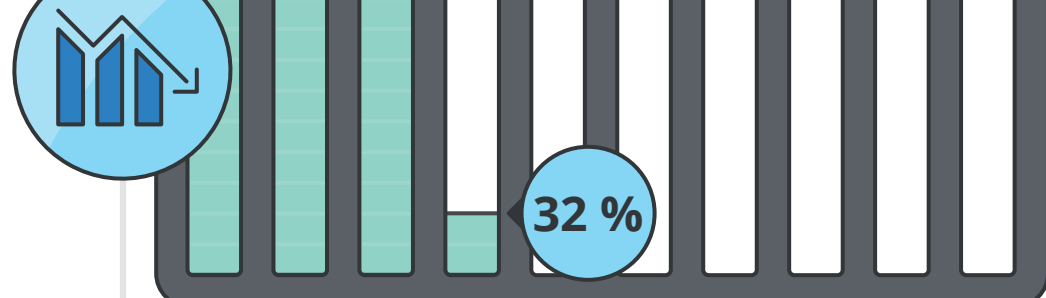
35 %

Über ein Drittel kann das vollständige Potenzial von Sicherheitstechnologien nicht nutzen, wodurch die Effektivität sinkt.



32 %

Ebenfalls fast ein Drittel berichtete von zunehmenden Abnutzungserscheinungen und mehr Fluktuation, wodurch die Situation noch verschärft wird.



Unterstützung für Ihre Sicherheitsprobleme

Die Implementierung von IoT-Kontrollmechanismen sowie für unternehmenseigene und BYOD-Geräte ist einfach. Zudem können CISOs zusammen mit den CIOs für mehr Sicherheit im Unternehmen sorgen. Was ist jedoch der beste Weg, um dieses Ziel zu erreichen? Ein in sich geschlossener Lösungsansatz für mehr Netzwerksicherheit mit folgenden Kriterien⁴:



Aruba ClearPass

Aruba ClearPass schließt diesen Kreislauf, sodass nur genehmigte, authentifizierte und einwandfreie IoT-, Unternehmens- und BYOD-Geräte in das Netzwerk gelangen können.

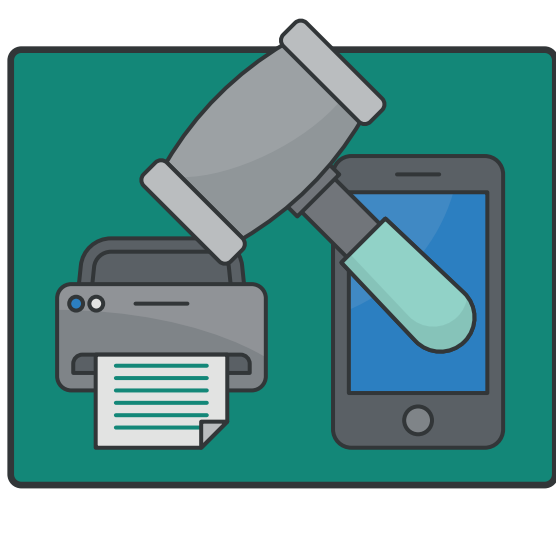
1



IDENTIFIZIEREN

von Geräten im Netzwerk: Anzahl der Geräte, Art der Vernetzung und installiertes Betriebssystem.

2



UMSETZEN

präzise formulierter Richtlinien für ordnungsgemäßen Benutzerzugriff, unabhängig von Benutzer, Gerätetyp oder Standort.

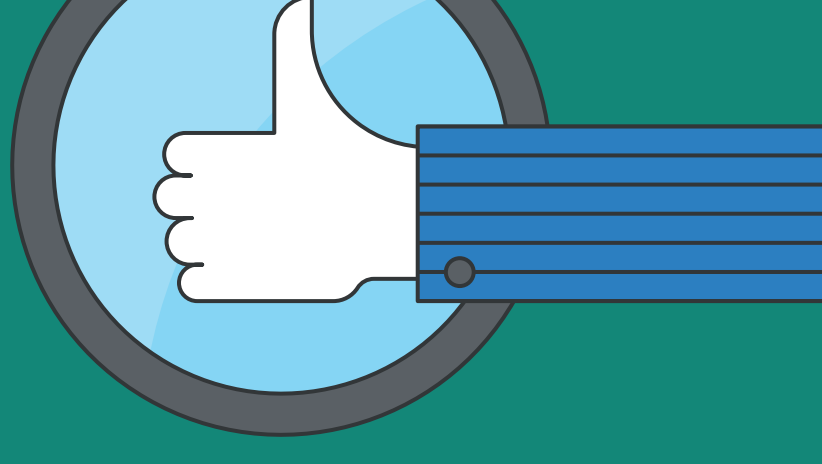
3



SCHÜTZEN

von Ressourcen mithilfe einer dynamischen Richtliniensteuerung und der Beseitigung von Bedrohungen, die auch Systeme von Drittanbietern einschließen können.

Reibungsloses Arbeiten



Aruba, ein Unternehmen von Hewlett Packard Enterprise, ist ein führender Anbieter von Netzwerklösungen der nächsten Generation.

Mit Aruba ClearPass ist Ihr Netzwerk sicher und effektiv, da die Erkennung von Bedrohungen und deren Behebung im Mittelpunkt stehen.

Wie sicher ist Ihr Unternehmensnetzwerk? Finden Sie es heraus – mit unserem Enterprise Security Assessment Tool.

RISIKEN ERMITTELN



QUELLEN:

- ¹ gartner.com/newsroom/id/3508917
- ² arubanetworks.com/solutions/internet-of-things/
- ³ engage.arubanetworks.com/LP_REG_510245507_510245507_ARUBA_WW_EN-US
- ⁴ arubanetworks.com/assets/wp/EP_ESG_HPE_Aruba_2017.pdf

Alle in diesem Dokument angeführten Statistiken sind allgemeiner Natur.