Ein Forrester Consulting
Thought Leadership-Dokument im
Auftrag von Infoblox

Juli 2020

Beschleunigung der Bekämpfung von IT-Sicherheitsrisiken mit Hilfe von DNS

Nutzen Sie DNS als die erste Verteidigungslinie in der IT-Security, um Angriffe zu erkennen, zu blockieren und zu untersuchen

FORRESTER®

Inhaltsverzeichnis

Projektleiter:
Sarah Brinks,
Senior Market Impact Consultant

Mitwirkende:
Forrester Research Group für Sicherheit und Risiken

ÜBER FORRESTER CONSULTING

Forrester Consulting bietet unabhängige und objektive forschungsbasierte Beratungsdienstleistungen, um Führungskräften den Erfolg in ihren Unternehmen zu sichern. Die Dienstleistungen von Forrester Consulting reichen von kurzen Strategieberatungen bis zu kundenspezifischen Projekten und bringen Sie direkt mit Analysten zusammen, die ihr Fachwissen gezielt auf Ihre jeweiligen unternehmerischen Herausforderungen anwenden. Weitere Informationen finden Sie unter forrester.com/consulting.

[E-47344]

FORRESTER®

Untersuchungen zu den IT-Bedrohungen dauern zu lange.

74 % der Sicherheitsteams verbringen mehr als 4 Stunden mit der Untersuchung eines einzelnen Bedrohungsereignisses.

Mehr Automatisierung ist erforderlich.

58 % der Führungskräfte in der IT-Security verwenden eine Mischung aus manuellen und automatisierten Prozessen zur Reaktion auf Vorfälle – nur 31 % sind fast vollständig automatisiert.

Zusammenfassung

Laut der Presse sind Kundendaten in der heutigen Wirtschaft wertvoller als Öl.[1] Wenn dies der Fall ist, muss der Schutz von Kundendaten für alle Unternehmen oberste Priorität haben. Das bedeutet, dass alle möglichen Zugänge zu Kundendaten gesichert sein müssen, unabhängig davon, wo diese Daten gespeichert werden. Das Domain Name System (DNS) ist ein grundlegender Netzwerkdienst, der sowohl für die Konnektivität als auch für die Sicherheit von entscheidender Bedeutung ist, da es eine Hintertür für unerlaubten Datentransfer sein kann. Es sollte daher als die erste Verteidigungsline in der IT-Security nicht übersehen werden, insbesondere in Zeiten von Krisen und Veränderungen, wie dem rasanten Anstieg von Heimarbeitern/Telearbeitern.

Im Januar 2020 beauftragte Infoblox Forrester Consulting mit der Bewertung der Nutzung von DNS bei der Erkennung bösartiger Angriffe und der Verhinderung von Datenverlust. Forrester führte eine repräsentative Online-Umfrage mit 203 führenden Experten von Unternehmen durch, die in der Regel führend bei den Best Practices für IT-Sicherheit und ein gutes Beispiel für diejenigen sind, die ihre eigene Situation in der IT-Security verbessern möchten. Wir haben US-amerikanische Sicherheits- und Risikoexperten von Unternehmen mit einem Jahresumsatz von 1 Mrd. US-Dollar oder mehr aus den Sektoren Regierung, Einzelhandel, Bildung, Gesundheitswesen und Finanzdienstleistungen befragt. Bei der Hälfte der Befragten handelt es sich um Chief Information Security Officers (CISO). Diese IT-Security-Experten nutzen DNS als wichtigen Bestandteil ihrer IT-Sicherheitsstrategie.

Führungskräfte im Bereich IT-Security verlassen sich bei drei Prioritäten auf DNS: 1) Bedrohungen so früh wie möglich in der Kill Chain erkennen und blockieren, 2) Bedrohungen untersuchen und darauf reagieren und 3) kompromittierte Geräte schnell identifizieren.

DIE WICHTIGSTEN ERGEBNISSE

- **DNS ist ein wichtiger Ausgangspunkt für die Untersuchung von Bedrohungen in der IT-Security.** DNS-Abfragen und -Antworten sind eine der drei wichtigsten Datenquellen, die SIT-Security Teams für die Suche nach Bedrohungen und Untersuchungen verwenden. IT-Security Analysten verlassen sich auf DNS, weil es böswillige Aktivitäten früher in der Kill Chain erkennt als andere Sicherheitstools. Außerdem erhalten Führungskräfte in der IT-Security die dringend benötigte Transparenz darüber, welche Geräte eine Verbindung zu schädlichen Zielen herstellen. Diese Transparenz ermöglicht es ihnen, diese Verbindungen zu trennen und ihre gesamte Infrastruktur zu schützen.
- **DNS füllt Lücken, die andere IT-Security Systeme nicht geschlossen haben.** Es gibt kein perfektes Sicherheitstool, das alle Ihre Probleme löst, aber es ist wichtig, Tools zu haben, welche mögliche IT-Security Sicherheitslücken schließt, die andere IT-Security Systeme nicht betrachten. Laut den befragten Führungskräften in der IT-Security liegt der Hauptvorteil der Verwendung eines internen DNS als IT-Security Protokoll Instanz zum Stoppen bösartiger Angriffe darin, Bedrohungen frühzeitig zu erkennen, die sonst nicht von anderen Sicherheitstools erkannt werden würden, zum Beispiel DNS-Tunneling/Datenexfiltration, Domain-Generation-Algorithmen (DGAs) und Look-Alike-Domain-Angriffe.
- **Die Mehrheit der Führungskräfte in der IT-Security möchte den ROI für Investitionen in IT-Security verbessern.** 56 Prozent der Führungskräfte in der IT-Security nannten den verbesserten ROI im Bereich IT-Security als hilfreichsten Vorteil für ihr Unternehmen. Im Zuge immer höherer Investitionen in IT-Security Tools in den letzten 10 Jahren möchten Führungskräfte in der IT-Security sehen, welchen ROI sie mit vorhandenen Investitionen erzielen können, bevor sie das Budget für weitere Tools und Technologien genehmigen.

FORRESTER®

DNS ist von entscheidender Bedeutung, um die Top Prioritäten in der IT-Security zu adressieren.

Führungskräfte in der IT-Security wissen, dass die Aufrechterhaltung des Kundenvertrauens für ihr Unternehmen von entscheidender Bedeutung ist. Der schnellste Weg, dieses Vertrauen zu verlieren, ist der Verlust und der Mißbrauch von Kundendaten. Wirklich kundenorientierte Führungskräfte in der IT-Security nutzen jedes ihnen zur Verfügung stehende Tool, um Bedrohungen frühzeitig zu erkennen und zu blockieren, IT-Bedrohungen zu untersuchen und darauf zu reagieren und kompromittierte Geräte schnell zu identifizieren. Bei der Befragung von 203 Führungskräften in der IT-Security haben wir die einzelnen Prioritäten untersucht:

ERKENNUNG

- **Das Erkennen kompromittierter Geräte beginnt mit DNS.** Die aktuellen Netzwerkumgebungen bergen mehr Risiken als je zuvor in jüngster Zeit. Mit dem Aufkommen der COVID-19-Pandemie und der anschließenden allgemeinen Neuausrichtung des Geschäftsbetriebs für alle Unternehmen öffnen sich IT-Sicherheitslücken. Immer mehr Mitarbeiter arbeiten von zu Hause aus mit ihren eigenen Geräten, sie schließen also zum Beispiel Internet-of-Things (IoT)-Geräte ohne die richtigen Sicherheitsmaßnahmen an, und IT-Security Teams müssen in der Lage sein, diese Geräte schnell zu identifizieren und zu reagieren, wenn diese kompromittiert werden. Unsichere Netzwerke, Geräte und Internetzugang gefährden Kundendaten. DNS-Abfragen und Antwortdaten sind eines der drei wichtigsten Tools, mit denen Unternehmen kompromittierte Geräte schnell identifizieren können. Die beiden wichtigsten Tools sind IPAM-Daten (IP Address Management) (67 %) und Netzwerkgeräteprotokolle (62 %).
- **Die Herausforderung der Datenexfiltration geht weiter.** Es war nie einfach, die Exfiltration von IT-Daten zu stoppen. In extremen Fällen können Angreifer Daten über DNS herausfiltern, allerdings ist es viel wahrscheinlicher, dass Angreifer gestohlene Daten über HTTP/HTTPS oder FTP hochladen. Im letzteren Fall hat das angegriffene Unternehmen Glück, wenn die DNS-Anforderung, die der Exfiltration von IT-Daten vorausgeht, auf einer öffentlichen IOC-Liste (Indicator of Compromise) steht.
- **Führungskräfte in der IT-Security erhalten aus DNS-Untersuchungen einen tiefen Einblick in die Art der IT-Angriffe.** Bei einem Angriff/einer Infektion benötigen die Ermittler Tools, die einen ganzheitlichen Überblick über das Ausmaß und die Schwere der Bedrohung bieten. DNS-Domain-/Adressuntersuchungen sind eines der zwei wichtigsten Tools, mit denen Ermittler feststellen können, wer in ihrem Unternehmen von einem Angriff/einer Infektion betroffen ist. Tatsächlich werden DNS- und Malware-Analysen als die wichtigsten Tools zur Identifizierung der Daten und Systeme, auf die der Angreifer Zugriff hat, genannt. DNS hilft Ermittlern außerdem zu bestimmen, auf wie viele Informationen der Angreifer Zugriff hatte.[2]

DNS ist ein wichtiger Kontrollpunkt für Bedrohungen.

69 % der Führungskräfte in der IT-Security nutzen DNS als Kontrollpunkt zur Abwehr von Angriffen.

BEDROHUNGEN BLOCKIEREN

- **DNS ist ein Top-3-Sicherheitskontrollpunkt für die Abwehr von Angriffen.** DNS-Filter/Firewalls wurden direkt hinter sicheren Web-Gateways/Proxy- und Intrusion Detection/Prevention-Systemen platziert, die IT-Security Teams zur Abwehr von Angriffen nutzen. 66 % der Führungskräfte in der IT-Security gaben tatsächlich an, dass DNS es ihnen ermöglicht, Malware-Aktivität früher in der Kill Chain zu erkennen, wodurch sich die Belastung ihrer Abwehrmaßnahmen reduziert.
- **Drei von vier Führungskräften in der IT-Security nutzen DLP-Lösungen (Data Loss Prevention) zum Schutz von Daten.** Mehr als drei Viertel der Befragten verwenden DLP-Lösungen, um die Sicherheit ihrer Kundendaten zu gewährleisten. Die verbleibenden 24 % der Führungskräfte in der IT-Security nutzen andere Lösungen, wie Firewalls der nächsten Generation, sichere Web-Gateways und Cloud Access Security Broker (CASB), zum Schutz ihrer Daten.

UNTERSUCHUNG UND REAKTION AUF BEDROHUNGEN

94 Prozent der Führungskräfte in der IT-Security in unserer Studie gaben an, DNS als Ausgangspunkt für ihre Bedrohungsuntersuchungen in Betracht gezogen zu haben oder zu ziehen. DNS spielt eine entscheidende Rolle bei der Beschleunigung der Reaktion auf IT-Security Vorfälle auf allen Geräten im Unternehmen im Hauptnetzwerk, in Zweigstellen und an mobilen Arbeitsstandorten sowie im gesamten IoT. Ein unternehmensweiter Ansatz zur gemeinsamen Nutzung der Threat Intelligence wird von mehr als einem Drittel der Führungskräfte in der IT-Security als entscheidend angesehen, während weitere 45 % der Meinung sind, dass dies ihrem Unternehmen zugute kommen würde.

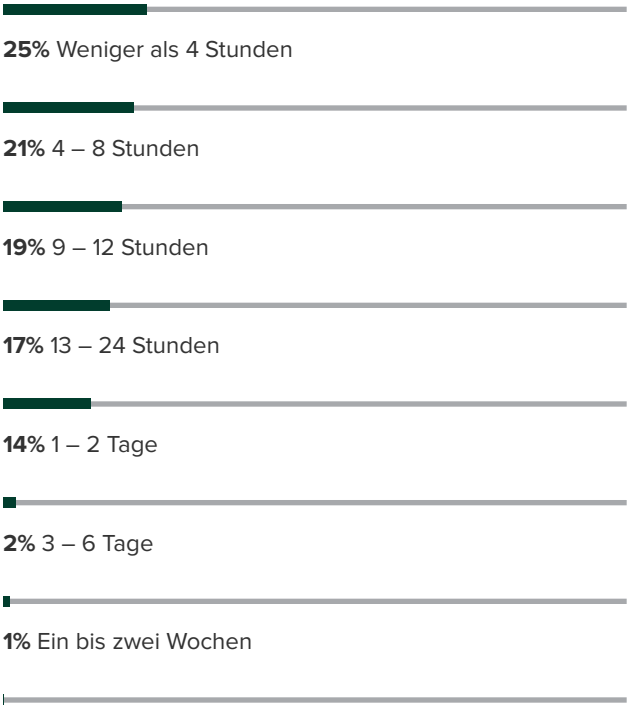
- **Selbst Führungskräfte in der IT-Security können nur ein bis zwei Untersuchungen pro Tag durchführen.** Etwa die Hälfte (46 %) der Führungskräfte in der IT-Security in unserer Studie gab an, dass es durchschnittlich 1 bis 8 Stunden dauert, eine Bedrohung zu untersuchen. Das entspricht im Durchschnitt etwa einer oder zwei vollständigen Untersuchungen pro Tag. Schnellere Reaktionszeiten erfordern Integrationen und automatische Datenfreigabe zwischen IT-Security Tools, die sowohl von qualifizierten und geschulten Mitarbeitern als auch durch präzise Prozesse unterstützt werden (siehe Abbildung 1).
- **Automatisierung ist entscheidend für die Verbesserung der Reaktionsraten bei Vorfällen.** Fast 60 % der leitenden Führungskräfte in der IT-Security verfügen über eine Mischung aus manuellen und automatisierten Prozessen zur Reaktion auf IT-Security Vorfälle. Nur 31 % der befragten Führungskräfte in der IT-Security gaben an, dass ihre Prozesse zur Reaktion auf Vorfälle nahezu vollständig automatisiert sind. Diese Führungskräfte sind sich bewusst, dass jeder Teil des Prozesses, der automatisiert werden kann, automatisiert werden sollte, um die Geschwindigkeit und Genauigkeit der Reaktionen auf IT-Security Vorfälle zu verbessern. Mithilfe von Tools zur Sicherheitsorchestrierung, Automatisierung und Reaktion (SOAR) automatisieren die meisten Befragten ihren Reaktionsprozess auf Vorfälle, während andere speziell Tools auswählen, die Automatisierung beinhalten oder selbst erstellte Skripte verwenden. Selbst erstellte Skripte werden am häufigsten von der Regierung/Bundesbehörden verwendet. Im Laufe der Zeit wurden Tausende von Skripten geschrieben, um verschiedene Teile des Prozesses zur Reaktion auf Bedrohungen zu adressieren, was langfristig zu einer Last für den Support werden kann.

DNS fördert effektivere Untersuchungen bei IT-Bedrohungen oder der Analyse von IT-Security Angriffen.

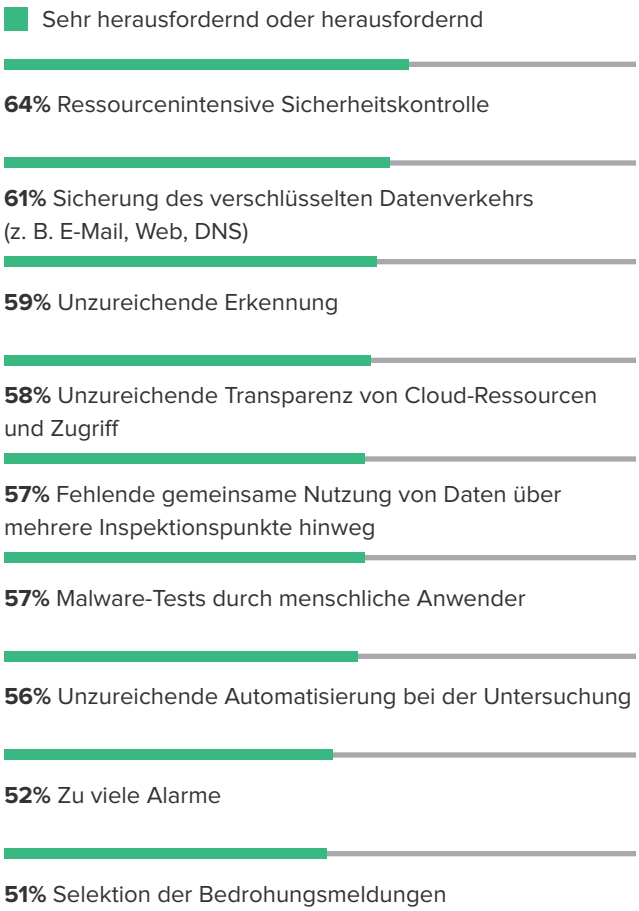
Führungskräfte in der IT-Security verwenden bei Untersuchungen zur Korrelation von Netzwerkprotokollen DNS-Daten zur Ermittlung der Gefährdung und Untersuchung ausgehender Ressourcen.

Abbildung 1

„Wie lange dauert es im Durchschnitt, bis Ihr Sicherheitsteam eine Bedrohung untersucht?“



„Wie herausfordernd sind die folgenden Faktoren für die Vermeidung und Untersuchung von Bedrohungen in Ihrem Unternehmen?

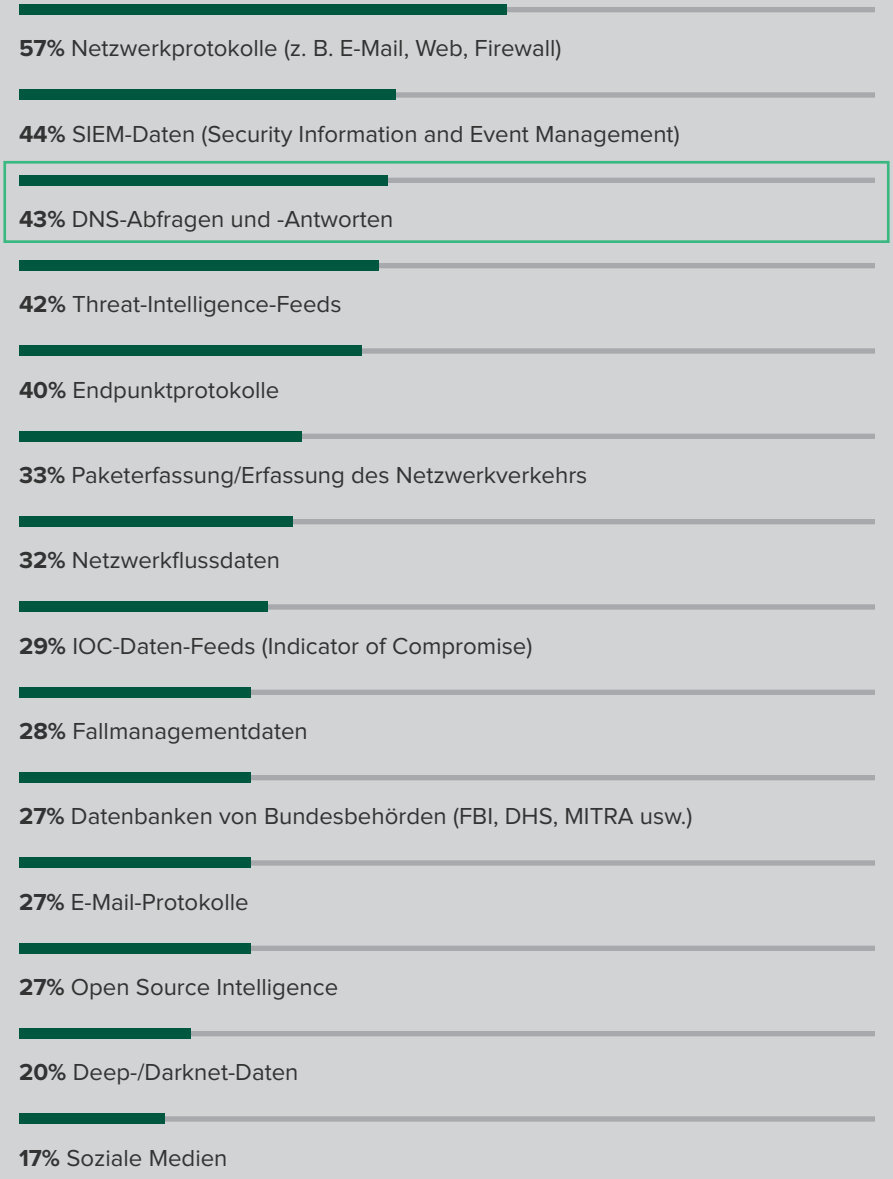


Basis: 203 US-Sicherheitsverantwortliche
Quelle: eine Studie von Forrester Consulting im Auftrag von Infoblox, April 2020

› **DNS ist eine der wichtigsten Datenquellen für die IT-Security Analysten.** 43 Prozent der Führungskräfte in der IT-Security verlassen sich bei der Durchführung von Bedrohungsuntersuchungen auf DNS-Abfragen und -Antworten. Dies bedeutet, dass DNS nach Netzwerkprotokollen (57 %) und SIEM-Daten (Sicherheitsinformationen und Ereignismanagement) (44 %) eine der drei wichtigsten Datenquellen (43 %) für IT-Security Analysten ist (siehe Abbildung 2). DNS ist ein wichtiger Teil der Sicherheitsstrategie von Führungskräften in der IT-Security, es schützt Firmen vor Bedrohungen, die andere Sicherheitstools nicht erkannt haben könnten, und ermöglicht es IT-Security Analysten, herauszufinden, welche Geräte Verbindungen zu bösartigen Zielen angefordert haben.

Abbildung 2

„Auf welche der folgenden Datenquellen verlassen sich Ihre Sicherheitsteams, um eine Untersuchung von aktuellen Bedrohungen durchzuführen?“



Basis: 203 US-Sicherheitsverantwortliche
Quelle: eine Studie von Forrester Consulting im Auftrag von Infoblox, April 2020

FORRESTER®

IT-Security Analysten-Teams müssen Alleskönner sein

Laut der Forrester Analytics Global Business Technographics® Security Survey 2019 erlebten 43 % der Befragten in den USA während der letzten 12 Monate einen oder mehrere Verstöße, die sensible Daten kompromittierten.[3] 22 Prozent der angegriffenen Unternehmen gaben an, dass der Angriff über DNS erfolgte. Die hohe Anzahl von Bedrohungen aus so vielen Quellen und von so vielen Angreifern bedeutet, dass Führungskräfte in der IT-Security vielen Herausforderungen gegenüber stehen:

- **IT-Security Analysten Teams sind bei Untersuchungen von der massiven Anzahl von Faktoren überfordert.** Ohne unmittelbaren und ungehinderten Zugriff auf alle forensischen Ressourcen haben IT-Security Analysten oft das Gefühl, dass die Erkennung von Bedrohungslagen unzureichend ist. Sie benötigen klare Transparenz und Zugriff auf Private und Public Clouds. Darüber hinaus haben IT-Security Analysten mit verschlüsseltem Datenverkehr über E-Mail, das Internet und bald auch DNS zu kämpfen.
- **Überlastung hat sich eingestellt, und die Automatisierung hinkt hinterher.** Die Menge an Warnungen, die IT-Security Analysten wöchentlich und sogar täglich handhaben, kann erschreckend hoch sein. 52 Prozent der Führungskräfte in der IT-Security gaben an, dass zu viele Warnungen oder das Ignorieren der vielen Alarmmeldungen eine Herausforderung darstellen. Hinzu kommt, dass für 51 % das Erkennen von relevanten Alarmmeldungen zu Bedrohungen eine Herausforderung darstellt. Wie gehen Sie mit dieser Situation um? Automatisierung ist die direkte Antwort, aber selbst unter den führenden der befragten Führungskräfte in der IT-Security gaben 56 % an, dass ihre Unternehmen nicht ausreichend automatisiert sind, um auf IT-Bedrohungen zu reagieren.
- **Möglichen Zugriff auf böswillige Websites für mobile Mitarbeiter während einer Krise erkennen und blockieren.** Als die COVID-19-Pandemie im März 2020 die USA erheblich traf, begannen Unternehmensmitarbeiter in Nordamerika zunehmend von zu Hause/mobil zu arbeiten. Mitarbeiter, die noch nie im Home Office arbeiten mussten, waren plötzlich gezwungen, einen Weg finden, von zu Hause aus zu arbeiten und gleichzeitig sensible Kundendaten zu schützen. Unsere Umfrage wurde hauptsächlich Ende März durchgeführt, als die Pandemie in den USA erst in den Anfangsphasen war. Schon damals waren Führungskräfte in der IT-Security der Ansicht, dass sie bei der Erkennung und Blockade von IT-Bedrohungen für ihre mobilen Mitarbeiter am wenigsten effektiv waren (siehe Abbildung 3). 2020 wurden Führungskräfte in der IT-Security auf die Probe gestellt, als sie lernen mussten, mobile Geräte und Netzwerke von Mitarbeitern umfassender zu sichern als in der Vergangenheit. Führungskräfte in der IT-Security, die schnell und entschlossen handeln können, werden langfristig gewinnen.

Laut der Forrester Analytics Global Business Technographics Infrastructure Survey 2019 können Unternehmen über 500.000 Tablets und mehr als 2 Mio. Laptops besitzen, was viele potenzielle Infektions- und Angriffspunkte schafft.

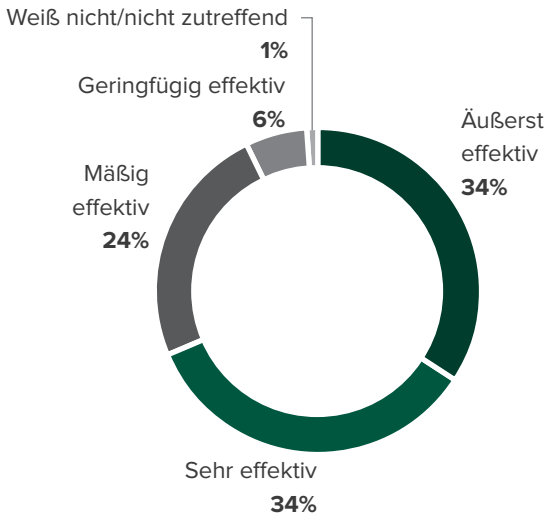
DNS ist für den Schutz vor Bedrohungen von entscheidender Bedeutung.

66 % der Führungskräfte in der IT-Security gaben an, dass DNS in der Lage ist, Bedrohungen abzufangen, die andere Sicherheitstools nicht aufhalten können.

Abbildung 3

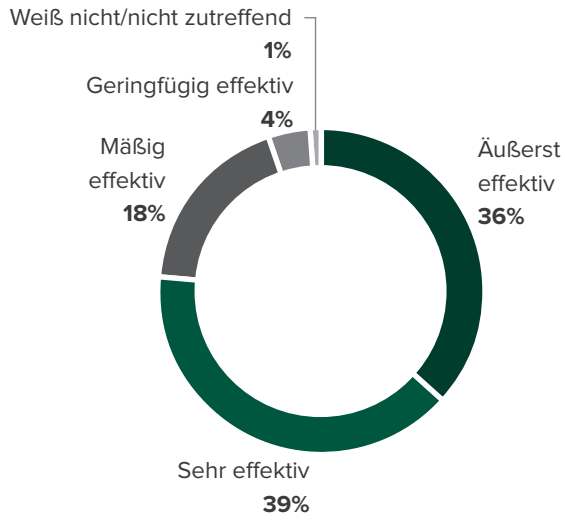
„Wie effektiv sind Sie bei der Erkennung von Zugriff auf schlechte Ziele und bösartige Websites an den folgenden Standorten?“

STANDORTE MOBILER MITARBEITER



„Wie effektiv sind Sie beim Blockieren des Zugriffs auf schlechte Ziele und bösartige Websites an den folgenden Standorten?“

STANDORTE MOBILER MITARBEITER



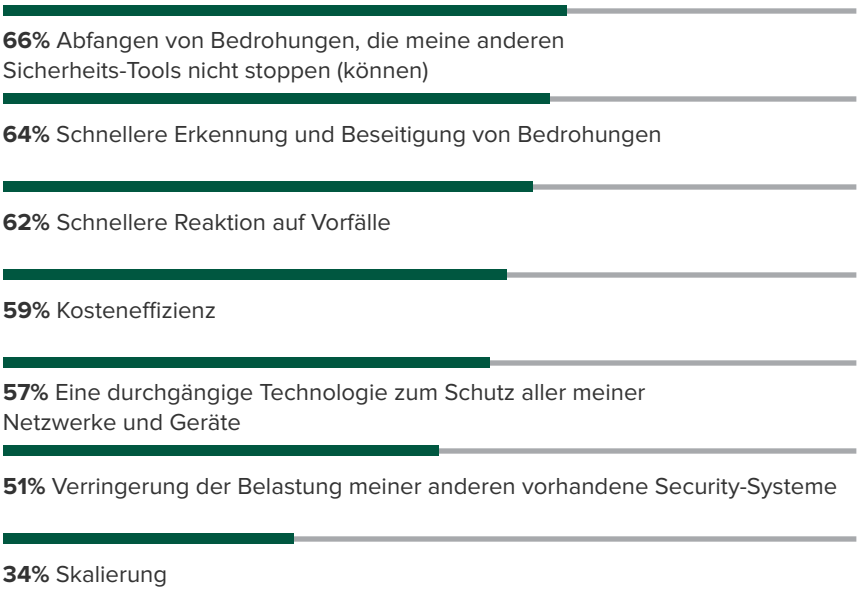
Basis: 203 US-Sicherheitsverantwortliche
Quelle: eine von Forrester Consulting im Auftrag von Infoblox durchgeführte Studie, April 2020. Hinweis: Prozentsätze ergeben aufgrund von Rundungen evtl. nicht 100.

- **Die Verwendung von internem DNS als IT-Security Layer löst wichtige Herausforderungen in der IT-Security.** 66 Prozent der Führungskräfte in der IT-Security gaben an, dass DNS in der Lage ist, Bedrohungen frühzeitig abzufangen, die andere Sicherheitstools nicht erkennen können. DNS hilft auch, die Reaktionszeiten bei IT-Security Vorfällen zu beschleunigen, was die Behebung von Bedrohungen beschleunigt. DNS unterstützt die Deception Technologien eines Unternehmens, die Angreifer beim ersten Durchdringen abfangen können; dieselbe Technologie kann genutzt werden, um Hosts auf spezielle Inspektionszonen umzuleiten, wenn sie Ressourcen von einer unbekannten Stelle anfordern. Mehr als ein Drittel der Unternehmen gab an, dass die Verwendung eines internen DNS als IT-Security Layer ihnen helfen kann, bösartige Angriffe im großen Stil zu stoppen (siehe Abbildung 4).
- **Führungskräfte in der IT-Security müssen sich den spezifischen Herausforderungen von COVID-19 stellen.** Unternehmen wurden zu einem beispiellosen Experiment mit neuen Arbeitsplatzmodellen wie Home-Office gezwungen, das scheinbar kein Ende hat. Bis ein Impfstoff auf breiter Basis verfügbar ist, wird ein Teil der Belegschaft immer außerhalb des Unternehmensnetzwerkes arbeiten.[4] Neben der viel höheren Anzahl mobiler Arbeitskräfte müssen Führungskräfte in der IT-Security auch die zusätzlichen Herausforderungen angehen, die COVID-19 zu Tage gebracht hat. Aufgrund der reduzierten Anzahl von Mitarbeitern vor Ort mussten viele Führungskräfte in der IT-Security Automatisierungslösungen finden, um Personallücken zu schließen und den Zugriff auf die Cloud und ihre Nutzung kontinuierlich zu überwachen. Vielen Unternehmen fehlen die Tools/Software, um ihre mobilen Mitarbeiter umfassend zu unterstützen. Anderen Unternehmen, insbesondere solchen in ländlichen Gebieten, fehlt die Internetbandbreite, um ihren Bedürfnissen gerecht zu werden. Böswillige Angreifer starten immer mehr Phishing- und Social Engineering-Angriffe und nutzen Schwachstellen in Collaboration-Tools – seien Sie also stets auf der Hut.[5]

FORRESTER®

Abbildung 4

„Welche Vorteile würden Sie von der Verwendung von internem DNS als Security Protokoll-Schicht erwarten, um bösartige Angriffe zu stoppen?“

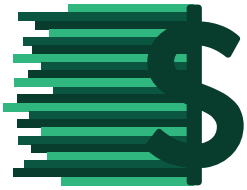


Basis: 203 US-Sicherheitsverantwortliche
Quelle: eine Studie von Forrester Consulting im Auftrag von Infoblox, April 2020

ROI-Anforderungen gerecht werden und den Kontext zu möglichen IT-Bedrohungen bekommen

Die Führungskräfte in der IT-Security stehen vor der Herausforderung, zu formulieren, welche Projekte den größten Nutzen für ihr Unternehmen generieren. Sie haben zudem oft Schwierigkeiten, bestehende Budgets zu rechtfertigen. Durch die Nutzung von Partnern, die die Leistung messen und den Kontext für IT-Bedrohungen bereitstellen können, sind Führungskräfte in der Lage, Budgets besser zu rechtfertigen und in marktführende Tools und Technologien zu investieren. In dieser Studie haben wir Folgendes festgestellt:

- **Selbst Top-Führungskräfte in der IT-Security suchen nach zusätzlichen Dienstleistungen.** Wir haben uns für diese Studie an Top-Führungskräfte in der IT-Security gewandt, aber selbst leitende Experten aus Unternehmen, die in der Regel führend bei Best Practices im Bereich Sicherheit sind, wissen, dass sie sich weiter verbessern können. Führungskräfte in der IT-Security sind intensiv auf der Suche nach einem Service, der ihren ROI im Bereich Sicherheit verbessert. Durch die Einsparung von Geld bei der Analyse von IT-Security Angriffen können sie weiter in Innovationen, bessere Technologien und die Einstellung/Schulung von Personal investieren. Darüber hinaus suchen sie nach Services zur kontinuierlichen Überwachung, die ihre Herausforderungen im Hinblick auf die Transparenz erfüllen. Sie möchten auch bei der Automatisierung häufig auftretender und sich wiederholender Sicherheitsaufgaben helfen, da dies zu Kosteneinsparungen führt. Und im Hinblick auf die Zukunft kann Automatisierung nur ein wichtiges Hilfsmittel für die Belegschaft sein, die sich gerade erst in die Telearbeit auf permanenter oder semi-permanenter Basis einfindet.

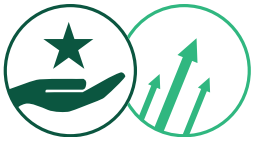


ROI ist am wichtigsten.

56 Prozent der Führungskräfte in der IT-Security nannten den verbesserten ROI im Bereich Sicherheit als hilfreichsten Service für ihr Unternehmen.

FORRESTER®

- **Führungskräfte in der IT-Security suchen nach einem detaillierteren Kontext für die Erkennung von IT-Bedrohungen.** Die Führungskräfte in der IT-Security in unserer Studie machten klar, dass sie eine bessere Threat Intelligence als die wichtigste Ressource zur Verbesserung der allgemeinen IT-Sicherheitsfunktionen ihrer Unternehmen einstuften (siehe Abbildung 5). Eine Schlüsselkomponente zur Verbesserung dieser Funktionen ist ein besseres Verständnis zur Erkennung von spezifischen IT-Bedrohungen. Führungskräfte erwarten von ihren Anbietern, dass sie sowohl den Kontext der einzigartigen IT-Bedrohungen für ihre Umgebung als auch die Komplexität ihres Unternehmens verstehen. Durch das Wissen, wonach sie suchen müssen, können IT-Security Analysten effektiver auf Sicherheitsverstöße reagieren, Bedrohungen schneller erkennen und teamübergreifend besser zusammenarbeiten. Kontextbezogene Informationen in Warnmeldungen können den Unterschied zwischen sofortiger und langwieriger Abwehr von IT-Angriffen/IT-Bedrohungen ausmachen.
- **Mobile Mitarbeiter benötigen ein höheres Maß an Threat Intelligence.** Inmitten der Coronavirus-Pandemie möchten oder verlangen viele Unternehmen, dass Büromitarbeiter von zu Hause aus arbeiten. Millionen von Mitarbeitern, die sich von Arbeitsplätzen in Unternehmensnetzwerken aus angemeldet haben, melden sich jetzt von zu Hause oder anderen Orten in öffentlichen Netzwerken an. Stärkere Authentifizierung und VPNs, die früher stets nur für einige Mitarbeiter erforderlich waren, werden jetzt zum Einstiegspunkt für Ihre gesamte Belegschaft.[6] Es wird erwartet, dass viele Arbeitnehmer für den Rest des Jahres 2020 zu Hause bleiben, einige werden sogar nie wieder ins Büro zurückkehren. Führende Unternehmen bieten ihren Mitarbeitern mehr Flexibilität bei der externen Arbeit. Unsere Studie ergab jedoch, dass es selbst führenden IT-Security Experten schwer fällt, gefährliche und böswillige Websites an Standorten mobiler Mitarbeiter zu erkennen und zu blockieren. Führungskräfte müssen schnell handeln, um DNS als Basis-Tool zur Bedrohungsanalyse zu nutzen und damit die Reaktion auf Vorfälle zu beschleunigen, Inventar zu erkennen und zu verwalten und ihre Strategie für die IT-Sicherheit für eine schnellere Behebung von IT-Bedrohungen zu optimieren.

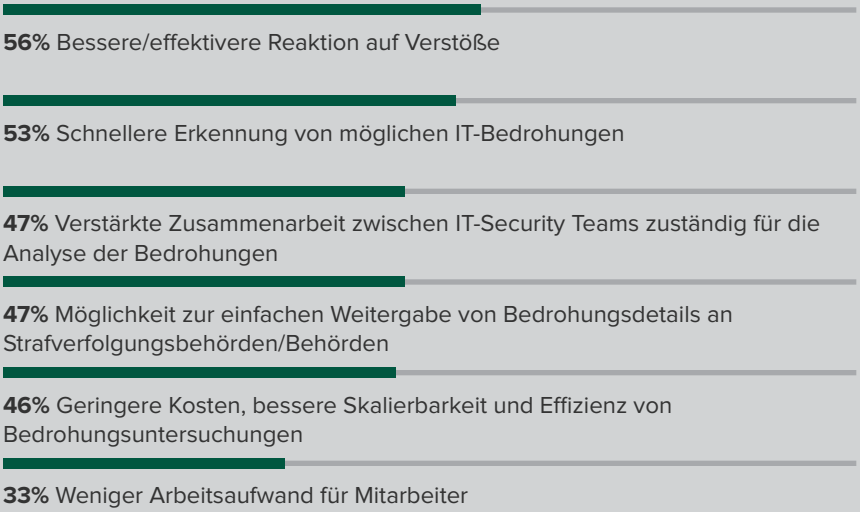


Ein klarer Kontext fördert eine effektive Reaktion bei Bedrohungen für die IT-Security.

Die Hälfte der Führungskräfte in der IT-Security betrachtet mehr/besseren Kontext als treibenden Faktor für Effizienz bei Erkennung, Reaktion auf Sicherheitsverletzungen und Zusammenarbeit.

Abbildung 5

„Welche Vorteile würden Sie erwarten, wenn Ihr Unternehmen mehr/besseren Kontext zu spezifischen IT-Bedrohungslagen hätte?“



Basis: 203 US-Sicherheitsverantwortliche
Quelle: eine Studie von Forrester Consulting im Auftrag von Infoblox, April 2020

FORRESTER®

Wichtige Empfehlungen

Die eingehende Umfrage von Forrester unter 203 führenden Sicherheits- und Risikoexperten in den USA über die Nutzung von DNS als grundlegenden IT-Security Layer ergab mehrere wichtige Empfehlungen:

Threat Intelligence im gesamten Unternehmen teilen. Die meisten von Forrester befragten Unternehmen sind sich einig, dass ein unternehmensweiter Ansatz zur gemeinsamen Nutzung von Threat Intelligence ein entscheidender Vorteil für ihr Unternehmen ist. Sicherheits- und Risikoexperten müssen die Threat Intelligence, die von ihren Top-Tier-Teams für Forensik und Sicherheitsanalyse verwendet werden, unternehmensweit bereitstellen, um den Wert dieser Informationen zu einem Zeitpunkt zu maximieren, an dem sie am effektivsten sein können.

Weitere Beschleunigung der Reaktion auf Vorfälle in der IT-Security. In den Jahren 2018 und 2019 gab es Rekordzahlen an hohen und kritischen Schwachstellen. Heute steht ein Sicherheitsmanagement-Team im Durchschnitt alle 9 Stunden einer neuen hohen oder kritischen Online-Schwachstelle gegenüber[7]. Gleichzeitig automatisieren Angreifer die Art Ihrer Angriffe auf bekannte IT-Schwachstellen, erweitern Ihre Möglichkeiten zu globalen Angriffen auf Unternehmen und zwingen diese zu entsprechenden Gegenmaßnahmen. Der Druck, auf IT-Security Vorfälle zu reagieren, und die Schwachstellen, die diese verursachen, treiben Unternehmen dazu, den schnellsten Weg zu gehen. Und für viele ist DNS dieser Weg.

Kontrolle über das Asset Discovery Management übernehmen. Modernes Asset-Management ist eines der schwierigsten Probleme, die es zu lösen gilt, unter anderem aufgrund der Leichtigkeit, mit der neue Geräte von Mitarbeitern, Remote-Teams und Partnern mit Unternehmensnetzwerken verbunden werden können. Die Erkennung von Ressourcen ist nach wie vor eine Herausforderung. Die integrierten DNS-Lösungen DHCP und IPAM können hier helfen, da sie die einzige Art von Kontrollpunkt sind, mit der die einzelnen Geräte garantiert interagieren können. Nutzen Sie IPAM-Daten, um gefährdete Geräte schnell zu identifizieren. Das Lifecycle-Management von Assets, von der Aufnahme bis zur Entsorgung, wird zu einer eigenen Disziplin.

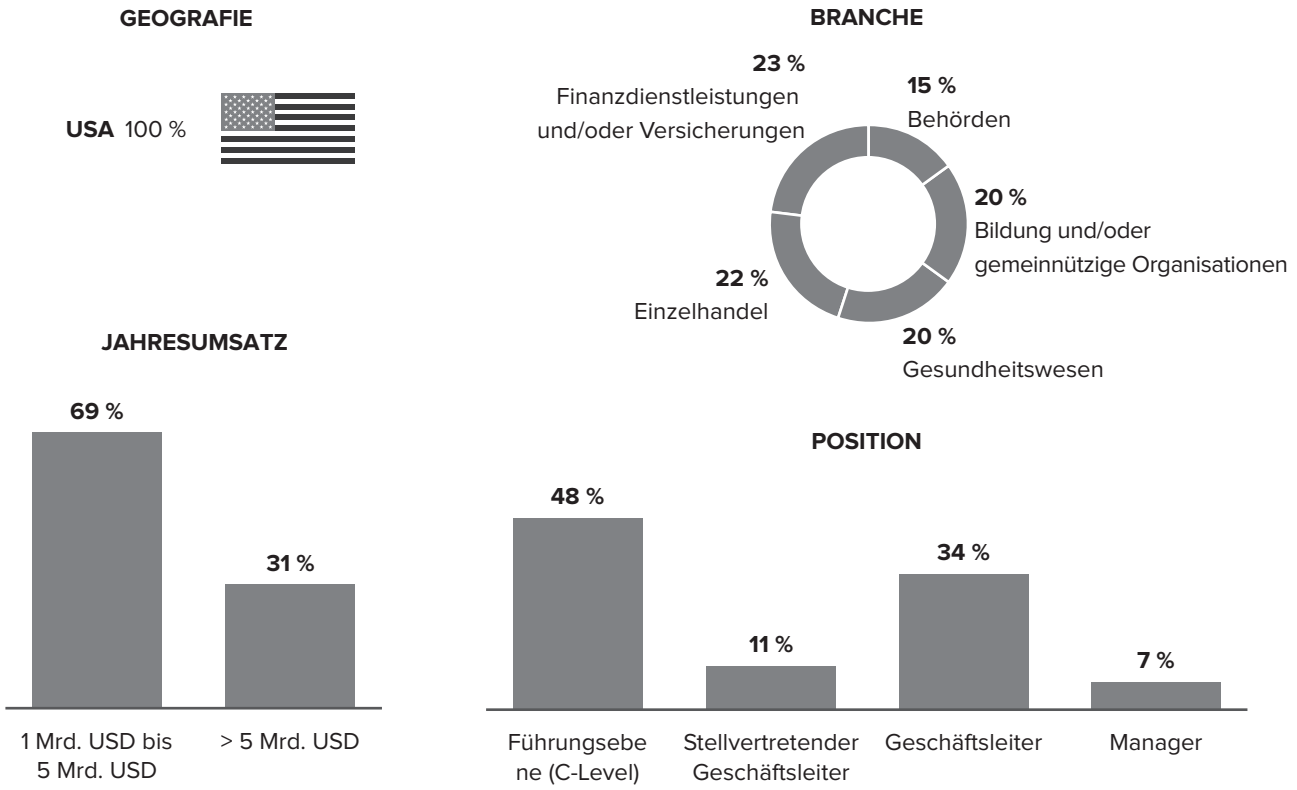
Taktische Erweiterung der vorhandenen Sicherheitsinfrastruktur. Die Architektur der IT-Sicherheitsstrategie ändert sich. Die Tendenz geht dahin, fast alle oder in einigen Fällen alle Sicherheitskomponenten über die Cloud bereitzustellen. Der Wettbewerb um das beste Sicherheitskonzept ist hart, aber es kann fünf Jahre oder mehr dauern, bis sich das dominante Design herausbildet. Vorsichtige Unternehmen können die Lebensdauer ihrer vorhandenen Sicherheitsinfrastruktur durch Optimierungen verlängern. Threat Intelligence über DNS kann hier eine große Rolle spielen, da „bekannte bösartige Verbindungen“ Unternehmen in die Lage versetzen, schneller günstige Entscheidungen zu treffen und nur die schwierigsten Inspektionen auf den vollen Stack zu übertragen, wo Sandboxing und menschliche Analyse das letzte Wort haben.

Weitere tiefgehende Verteidigung. Das Internet ist jetzt verschlüsselt; Anbieter von Network Analytics and Visibility (NAV) berichten Forrester informell, dass 72 % bis 95 % des Datenverkehrs in Unternehmensnetzwerken verschlüsselt ist. In vielen Unternehmen bleiben nur Metadaten wie DNS-Anforderungen als sichtbare Hinweise für Echtzeitanalysen erhalten. Sicherheits- und Risikoberufe werden weiterhin die bewährten DNS-Firewall- und Filtertechniken als erste Verteidigungslinie gegen Malware, Phishing und Ransomware nutzen. Angreifer wissen dies und haben Algorithmen kuratiert, um zufällige Pseudo-Domainnamen für C2-Operationen zu generieren, was zu einem Wettrüsten führt, das nur KI in Echtzeit bekämpfen kann.

Anhang A: Methodik

In dieser Studie führte Forrester eine Online-Umfrage unter 203 US-Sicherheitsverantwortlichen aus den Bereichen Finanzdienstleistungen, Gesundheitswesen, Bildung, Einzelhandel und Regierungsbehörden durch, um zu bewerten, wie sie DNS bei ihren Bedrohungsuntersuchungen verwenden. Den Befragten wurde als Dankeschön für die Teilnahme an der Umfrage ein Anreiz geboten. Die Studie begann im April 2020 und wurde im April 2020 abgeschlossen.

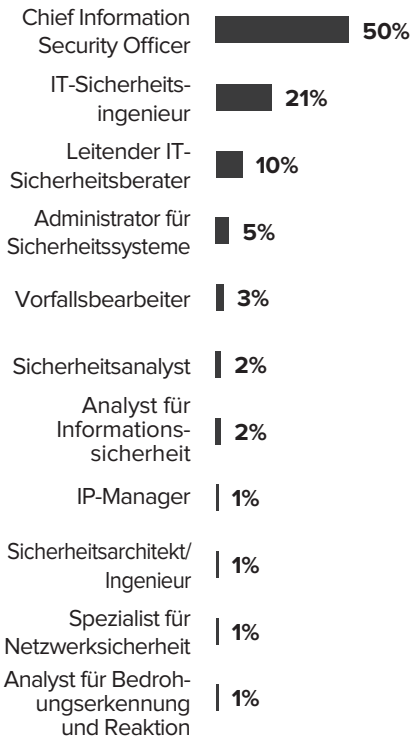
Anhang B: Demografische Daten



Basis: 203 US-Sicherheitsverantwortliche
Quelle: eine Studie von Forrester Consulting im Auftrag von Infoblox, April 2020
Hinweis: Die Prozentsätze ergeben aufgrund von Rundungen möglicherweise nicht 100.

FORRESTER®

ROLLE



ABTEILUNG

VERANTWORTUNG

	Strategie zur Sicherheits- und Risikobewertung	Threat-Intelligence -Strategie
Primär	79%	79%
Verantwortung teilen	17%	18%
Input geben und ausführen	3%	3%

Basis: 203 US-Sicherheitsverantwortliche
Quelle: eine von Forrester Consulting im Auftrag von Infoblox durchgeführte Studie, April 2020.
Hinweis: Prozentsätze ergeben aufgrund von Rundungen evtl. nicht 100.

Anhang C

FUSSNOTEN

[1] Quelle: Dan Gallagher, „Data Really Is the New Oil“ (Daten sind wirklich das neue Öl), The Wallstreet Journal, 9. März 2019.

[2] Quelle: Forrester Analytics Global Business Technographics Infrastructure Survey 2019.

[3] Quelle: Forrester Analytics Global Business Technographics Security Survey 2019.

[4] Quelle: „Collection: Learn To Support A Remote Workforce Permanently“ (Sammlung: So unterstützen Sie langfristige externe Mitarbeiter), Forrester (https://www.forrester.com/fn/37Kn3Q4mpMBdAxFZhMFbf1)..

[5] Quelle: „Address the Security and Privacy Challenges of Working from Home“ (Handhabung von Sicherheits- und Datenschutzherausforderungen bei der Arbeit im Home Office), Forrester (https://www.forrester.com/fn/21NX5awkIkxYASgFFz0Ejx).

[6] Quelle: Sean Ryan, „A Spike in Home Workers Raises MFA Resilience Questions“ (Eine rasante Erhöhung der Anzahl externer Mitarbeiter wirft Fragen zur MFA Resilience auf), Forrester Blogs, 17. März 2020, https://go.forrester.com/blogs/a-spike-in-home-workers-raises-mfa-resilience-questions/.

[7] Quelle: National Institute of Standards and Technology, CVSS Severity Distribution Over Time (CVSS-Schweregradverteilung im Laufe der Zeit) (https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time).

FORRESTER®