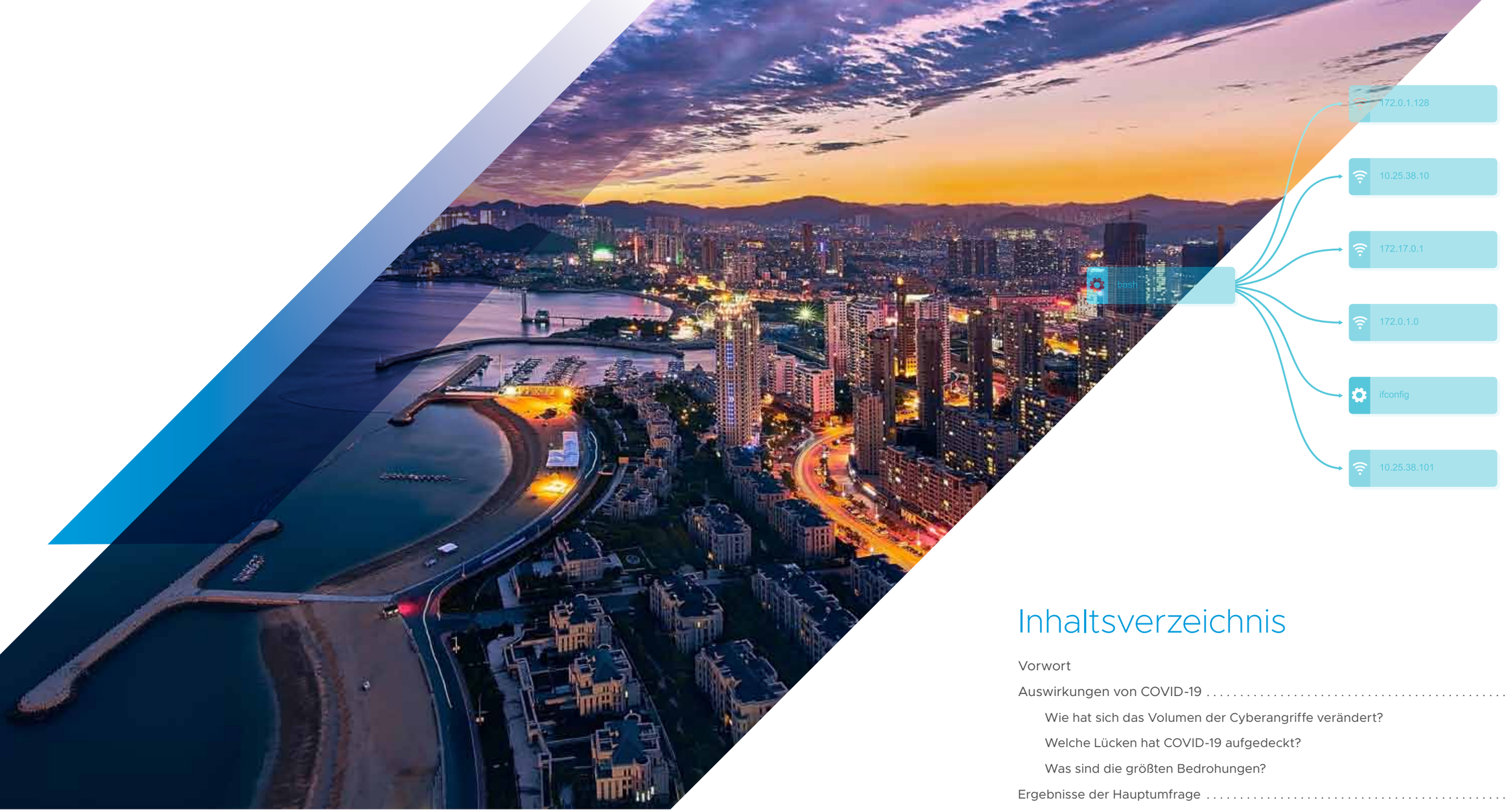
vmware Carbon Black

Deutschland Threat Report

Das Extended Enterprise in Gefahr

Juni 2020



Einführung

Diese Umfrage wurde durchgeführt, um die Herausforderungen und Probleme aufzudecken, mit denen deutsche Unternehmen im Zuge der ständig steigenden Cyberbedrohungen konfrontiert sind.

Der Report identifiziert Trends beim Hacking sowie bei Cyberangriffen und beleuchtet, welche finanziellen Folgen und Image-Schäden Datenschutzverletzungen für Unternehmen haben. Auch die Pläne deutscher Unternehmen zum Schutz von neuen Technologien, die Einführung von Frameworks für Cybersicherheit und die Komplexität ihrer aktuellen Umgebung zum Management von Cybersicherheit sind Gegenstand der Studie.

Inhaltsverzeichnis

CYBERANGRIFFE IN DEUTSCHLAND 2020: DIE AKTUELLE LAGE

Rick McElroy
Cyber Security Strategist, VMware Carbon Black

Vorwort:

Der dritte Threat Report für Deutschland ergab eine paradoxe Situation. 70 % der deutschen Sicherheitsexperten gaben an, dass die Zahl der Cyberangriffe auf ihre Organisation im letzten Jahr gestiegen sei. Das steht im Gegensatz zum globalen Trend: Im weltweiten Durchschnitt lag diese Zahl bei 90 %. Und es ist ein bemerkenswerter Rückgang gegenüber den 99 % vom Oktober 2019. Dennoch sind das keine guten Nachrichten, denn die Angriffe waren ausgereifter als je zuvor:

Insgesamt 82 % der Befragten sagten demnach, die Angriffe wären im letzten Jahr ausgefeilter geworden; 41 % der Befragten gaben sogar an, die Angriffe wären bedeutend ausgefeilter geworden.

Das stellt eine deutliche Steigerung dar im Vergleich zum Threat Report von Oktober 2019, wo lediglich 45 % angaben, Angriffe seien ausgereifter geworden. Die Steigerung bestätigt darüber hinaus einen Trend, den die VMware Carbon Black Threat Analysis Unit in ihren Studien feststellte: Demnach wenden die Angreifer immer ausgereiftere Taktiken an, da die Kommerzialisierung von Malware einer größeren Zahl an Cyberkriminellen ausgefeilte Angriffstechniken ermöglicht.

Die komplexen Angriffe überwinden erfolgreich Maßnahmen zur Cybersicherheit:

73 % der deutschen Unternehmen erlitten im letzten Jahr von Cyberangriffen verursachte Datenlecks. Je Unternehmen gab es durchschnittlich zwei Sicherheitsverletzungen.

Dennoch scheinen deutsche Unternehmen auf einem guten Weg zu sein: Seit dem ersten Threat Report entsprechen die 73 % dem geringsten Prozentwert bei Sicherheitsverletzungen. Auch die Anzahl der durchschnittlichen Sicherheitsverletzungen je Unternehmen ist am niedrigsten (Herbst 2019: 2,38 durchschnittlichen Sicherheitsverletzungen je Unternehmen).

Die häufigste Angriffsart stellen dateilose Angriffe dar (Living off the Land, PowerShell und WMI). Angreifer versuchen zudem vorwiegend, unbemerkt Netzwerkzugriff zu erhalten als Basis für weitere Aktivitäten und laterale Bewegungen. Im Zuge der Ursachenforschung für erfolgreiche Angriffe sollten Organisationen aber zunächst das Naheliegendste prüfen: So spielten in immerhin 37 % der Sicherheitsverletzungen Schwachstellen in Prozessen und veraltete Sicherheitsmaßnahmen eine Rolle.

METHODIK

VMware Carbon Black beauftragte das unabhängige Marktforschungsunternehmen Opinion Matters im März 2020 mit der Durchführung einer Umfrage. Befragt wurden 251 deutsche CIOs, CTOs und CISOs von Organisationen aus verschiedenen Sektoren u.a. Finanzdienstleister, Gesundheitswesen, Behörden, Einzelhandel, Industrie, Lebensmittel und Getränke, Zuliefererbetriebe, Professional Services sowie aus der Medien- und Entertainmentbranche. Der vorliegende dritte Threat Report für Deutschland von VMware Carbon Black baut auch auf den Reports vom Februar 2019 und Oktober 2019 auf. Die Umfrage in Deutschland ist Bestandteil eines weltweiten Forschungsprojekts, für das neben Deutschen auch IT-Führungskräfte aus Australien, Frankreich, Italien, Japan, Kanada, den Niederlanden, den Nordischen Ländern, Singapur, Spanien, den USA und dem Vereinigten Königreich befragt wurden.

82%

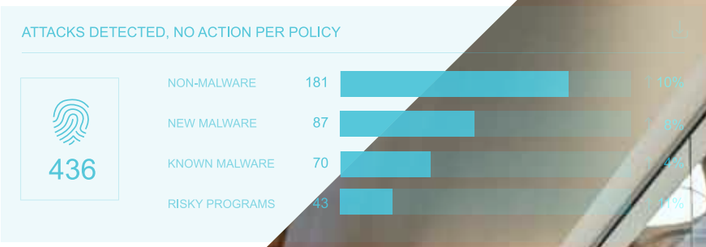
der Befragten sagten, die Angriffe wären im letzten Jahr ausgefeilter geworden.

73%

der deutschen Unternehmen erlitten im letzten Jahr von Cyberangriffen verursachte Datenlecks.

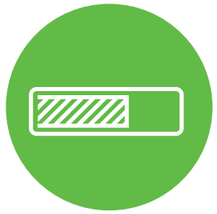
20%

Dateilose Angriffe standen in Deutschland mit einem Fünftel aller Angriffe an erster Stelle.



61%

KMUs meldeten einen durchschnittlichen Anstieg des Angriffsvolumens um 61 %. Sie waren damit im Vergleich zu kleineren und größeren Unternehmen am stärksten betroffen.



Risiko Lieferkette

KMUs befinden sich häufig in Lieferketten größerer Unternehmen und stellen so auch für diese ein Risiko dar.

51%

geben an, die Ausgaben für Sicherheit und Kontrollen im Rahmen von 5G zu erhöhen.

KMUs als Hauptbetroffene

Die Studie ergab, dass unterschiedlich große Unternehmen auch unterschiedlich stark bedroht sind. Am attraktivsten für Angreifer scheinen KMUs mit 501 – 1000 Mitarbeitern zu sein. Das sind Unternehmen, die einerseits in der Regel nicht mit größeren Organisationen vergleichbare Budgets oder interne Ressourcen für IT-Sicherheit besitzen, deren Daten und digitalen Assets andererseits aber immer noch ein lohnendes Ziel für Diebstahl oder Erpressung sind. Diese KMUS sehen sich im Vergleich zu kleineren und größeren Unternehmen signifikant mehr Angriffen und immer ausgereifteren Angriffen ausgesetzt.

Bei Unternehmen dieser Kategorie sind dateilose Angriffe der häufigste Angriffstyp. Dieser Typ macht bei KMUs 43 % der gesamten Angriffe aus. Nimmt man den Durchschnitt von Unternehmen aller Größenordnungen, beträgt der Anteil nur 20 %. Hier sollten die Alarmglocken läuten, und zwar nicht nur für Unternehmen im KMU-Segment. Denn die KMUs befinden sich häufig in Lieferketten größerer Unternehmen und stellen so ein beträchtliches Risiko als potenzielle Einfallstore für Island-Hopping-Angriffe dar. IT-Sicherheit bei Lieferanten und Sorgfaltspflicht müssen hohe Priorität erhalten, wenn Unternehmen die Risiken in den Griff bekommen wollen, die über ihre Lieferketten drohen.

Wachsende Budgets bei den meisten Unternehmen - doch werden diese Ausgaben strategisch oder taktisch eingesetzt?

Deutsche Sicherheitsexperten sind, wenn es um höhere Ausgaben für IT-Sicherheit geht, zurückhaltender als ihre internationalen Kollegen und schränken Ausgaben im Vergleich zu früheren Zeiträumen ein. Nur noch 86 % planen eine Erhöhung, was ein Rückgang gegenüber den 98 % vom letzten Threat Report bedeutet. Dies liegt auch unter dem weltweiten Durchschnitt von 96 %.

Eine zentrale Frage ist, wofür das Budget verwendet wird. Die Befragten unterstrichen, dass sich Threat Hunting auszahlt und sein Beitrag zur proaktiven Identifizierung von Angreifern, die sich bereits im System befinden, immer höher geschätzt wird. Es ist demnach wahrscheinlich, dass weiterhin Investitionen in diesen Bereich fließen. Doch wie sehen die Investitionen bei neu entstehenden Risiken aus?

Im Threat Report vom Oktober 2019 äußerten 99 % der Befragten aus Deutschland Sicherheitsbedenken hinsichtlich der digitalen Transformation und 5G. Geht es aber konkret um die Notwendigkeit von Ausgaben für IT-Sicherheit, so weichen die Meinungen voneinander ab. 51 % geben an, die Ausgaben für Sicherheit und Kontrollen zu erhöhen, während 42 % die Budgeterhöhungen nicht auf die Sicherheit im Bereich 5G konzentrieren werden.

Komplexe und unübersichtliche Multi-Technology-Umgebungen

Das liegt möglicherweise daran, dass die Verantwortlichen bereits auf eine Vielzahl von IT-Sicherheitstechnologien setzen. Befragte nutzen im Rahmen ihres IT-Sicherheitsprogramms durchschnittlich über elf verschiedene Konsolen oder Agents. Eine solche Vielfalt ist ein Indiz für IT-Sicherheitsumgebungen, die sich reaktiv weiterentwickelt haben. Das bedeutet, dass neuen Bedrohungen mit neuen Sicherheitslösungen begegnet wurde. Das führt zu Umgebungen, die aus Insellösungen bestehen, umständlich zu managen sind und es Angreifern leichter machen. Weil Cyberbedrohungen immer effektiver werden, ist es Zeit für Rationalisierung und klare Strategien für Sicherheitsmaßnahmen.

Unterschiedliche Bewertungen von Security Frameworks

Die Sichtbarkeit und Validierung der Sicherheitslage kann mithilfe des MITRE ATT&CK®-Frameworks – einer Bündelung kollektiven Wissens über Taktiken und Techniken, die Angreifer anwenden – deutlich verbessert werden. Jedoch bewerten Entscheider in Deutschland diese Herangehensweise noch unterschiedlich. 72 % kennen das MITRE ATT&CK® Framework, aber nur 35 % planen es zur Validierung ihrer Sicherheitslage zu verwenden. Das zeigt, dass noch Arbeit nötig ist, um dieses Framework als Standardwerkzeug für Unternehmen zu etablieren.

Risikofaktor Netzwerke

An erster Stelle der Sicherheitsrisiken stehen den Befragten zufolge Netzwerke. Über ein Drittel (37,5 %) geben an, dass diese das größte Sicherheitsrisiko darstellten. An zweiter Stelle folgen Workloads und Anwendungen, von denen einem Fünftel der Unternehmen zufolge (18 %) ein Sicherheitsrisiko ausgeht. Das erscheint im Kontext der Zunahme von Sicherheitsverletzungen in Verbindung mit Apps von Drittanbietern nicht überraschend und bedeutet im Vergleich zum Threat Report von Oktober 2019 eine Zunahme von 11 %. Da Unternehmen immer mehr Apps verwenden, um flexibler und produktiver zu werden, nimmt deren Sicherheit eine kritische Rolle ein.

72% vs 35%

72 % kennen das MITRE ATT&CK® Framework, aber nur 35 % planen es zur Validierung ihrer Sicherheitslage zu verwenden.

Auswirkungen von COVID-19

Während der ersten Phase dieses VMware Carbon Black Threat Reports war die Dynamik der COVID-19-Pandemie noch nicht absehbar. Bald wurde jedoch offensichtlich, dass die Auswirkungen der Krise auf die Cybersicherheit und den Bereich der Cyberbedrohungen im Report zwingend berücksichtigt werden müssen. Daher haben wir den Fragenkatalog ergänzt, um die direkten Auswirkungen der Krise zu verstehen und zu erfahren, wie sich die Sicherheitsexperten an das sich rapide wandelnde Szenario anpassen. Wir sind allen Personen dankbar, die in dieser schwierigen Phase Zeit in die Beantwortung der Fragen investiert haben. Die gewonnenen Informationen sollten wertvolle Erkenntnisse für weitere Maßnahmen zur Cybersicherheit bieten.

Wir hoffen, dass Sie unseren dritten Threat Report für Deutschland informativ und nützlich finden.

Ergebnisse im Kontext von COVID-19

Weltweite Befragung von März bis April 2020 mit 1002 Teilnehmern aus dem Vereinigten Königreich, USA, Singapur und Italien

Es wird oft gesagt, dass kein Plan den Kontakt mit dem Feind übersteht. Hier kam er aus einer gänzlich unerwarteten Richtung. Durch den plötzlichen weltweiten Trend hin zum Homeoffice nahmen auch Cyberangriffe zu und es kristallisierten sich besondere Schlüsselbereiche heraus, denen Sicherheitsexperten besondere Aufmerksamkeit widmen müssen. Unsere Analysen zu COVID-19 zeigen, dass die meisten Unternehmen eine größere Zahl an Cyberangriffe verzeichnen, weil die Mitarbeiter von zuhause aus arbeiten. Hinzu kommen die Schäden durch Malware, die im Zusammenhang mit COVID-19 steht.

Die eklatantesten identifizierten Lücken in den Disaster-Recovery-Plänen der Unternehmen betreffen einerseits die Kommunikation mit externen Parteien, z. B. Kunden, potenziellen Kunden und Zulieferern, andererseits IT-Abläufe und Herausforderungen rund um die Einrichtung von Remote-Arbeitsplätzen für Mitarbeitende und interne Kommunikation.

Wer die Multi-Faktor-Authentifizierung bislang vernachlässigt hat, bereut das inzwischen: Sie ist oft auf die Schnelle nicht umzusetzen; ihr Fehlen stellt für über ein Viertel der Teilnehmer weltweit die größte Sicherheitsbedrohung dar. Während wir uns auf die neue Normalität im Homeoffice und den damit einhergehenden Bedrohungen einstellen, sehen sich IT-Teams vor der Herausforderung, für gute Cybersicherheit auch die Homeoffices der Mitarbeiter schützen zu müssen.

“Das Fehlen der Multi-Faktor-Authentifizierung stellt für über ein Viertel der Befragten (29%) weltweit die größte Sicherheitsbedrohung während COVID-19 dar.“

Hat sich die Gesamtzahl der Cyberangriffe auf ihr System verändert, weil mehr Mitarbeitende von zu Hause aus arbeiten?

Ein erstaunlich hoher Anteil von 91 % aller global Befragten gab an, dass sich bei ihnen die Zahl der Cyberangriffe erhöht hat, weil Mitarbeiter von zuhause aus arbeiten.

7 % der Teilnehmer gaben an, dass diese Zunahme zwischen 50 % und 100 % lag. Knapp unter einem Viertel (24 %) gab an, dass das Angriffsvolumen zwischen 25 % bis 49 % angestiegen ist.

Drei von 1002 Personen gaben an, dass ihre Mitarbeitenden trotz der Krise nicht häufiger von zuhause aus arbeiteten als sonst.

Von den vier an der Studie beteiligten Ländern gaben die Befragten aus **Singapur** am häufigsten eine Zunahme der Angriffe an (93 %), gefolgt vom **Vereinigten Königreich** mit 92 %, **Italien** mit 90,5 % und schließlich den USA mit 88 %. Dabei gaben die Befragten aus Italien die höchste Zunahme bei den stark gestiegenen Angriffen zu Protokoll: 14 % sagten aus, dass die Angriffe um 50 % bis 100 % zugenommen hatten. Im Vergleich dazu weist das **Vereinigte Königreich** mit 2 % den niedrigsten Wert in der Kategorie starker Angriffszunahme auf. Die **USA** hatte die Spitzenposition in der Kategorie 25 % – 49 %, wobei 28 % der Befragten angaben, dass Angriffe in diesem Prozentbereich zugenommen hatten.

14,5 % der Unternehmen im Bereich **Medien und Entertainment** hatten eine Zunahme der Angriffe zwischen 50 und 100 % zu verzeichnen. Der **Einzelhandel** hatte mit 13 % in dieser Kategorie auch unter wesentlich mehr Angriffen zu leiden. 45 % der Befragten im Einzelhandel gaben an, dass Angriffe um 25 % bis 49 % zunahmen. Es folgte die **Fertigungsbranche** mit 33 %.

41 % der Unternehmen mit **501 – 1000** Mitarbeitenden meldeten starke Zunahmen der Angriffe um 25 % bis 100 %.

Nur etwa über ein Viertel (26 %) der Unternehmen **mit IT-Abteilungen von über 100** Mitarbeitenden stellten Zunahmen der Angriffe zwischen 50 % und 100 % fest.

18 % der Unternehmen mit IT-Abteilungen von **41 – 50** Mitarbeitenden gaben Zunahmen zwischen 50 und 100 % an.

91%

aller global Befragten gab an, dass sich bei ihnen die Zahl der Cyberangriffe erhöht hat, weil Mitarbeiter von zuhause aus arbeiten.

48%
der weltweit Befragten gab größere Lücken bei der Kommunikation mit externen Parteien.

Welche Lücken in der Disaster-Recovery-Planung Ihres Unternehmens deckte die Covid-19-Pandemie auf und als wie signifikant erwiesen sich diese Lücken in der gegenwärtigen Krise?

Fast die Hälfte (48 %) der weltweit Befragten gab größere Lücken bei der **Kommunikation mit externen Parteien** wie Kunden, potenziellen Kunden und Partnern an. Insgesamt meldeten 84 % Lücken bei der **Kommunikation mit externen Parteien** – die Lücken reichten dabei von schwerwiegend bis klein.

Über ein Drittel (35 %) meldete größere Lücken ihrer Disaster-Recovery-Planung **bei den IT-Abläufen** einschließlich Hardware- und Softwarebereitstellungen. Insgesamt meldeten 87 % größere und kleinere Lücken bei **IT-Abläufen.**

Knapp ein Drittel (32 %) der Befragten weltweit stellte bemerkenswerte Lücken fest im Hinblick auf Sichtbarkeit und Transparenz von **Bedrohungen für die Cybersicherheit.** Weitere 38 % entdeckten kleinere Lücken.

Mit Bezug auf die **Einbindung von Remote-Mitarbeitern** wiesen insgesamt über 85 % der Befragten auf Lücken hin. Über ein Viertel (28 %) der Befragten gaben sogar große bedeutende Lücken an.

Über ein Viertel (27,5 %) räumten schwere Probleme mit der Pandemie bei der **Kommunikation mit Mitarbeitern** ein und insgesamt 78,2 % gaben an, dass diese entweder klein oder sehr bedeutend waren.

Mit Bezug auf **Disaster-Recovery-Pläne** gab ein Drittel (33 %) der Befragten sehr große Lücken an und 88 % verwiesen auf diverse Unregelmäßigkeiten.

Fünf Befragte von 1002 haben sich gegen die Beantwortung dieser Fragen entschieden und gaben an, dass im Zusammenhang mit der Pandemie COVID-19 keine Lücken bei der Disaster-Recovery-Planung ihres Unternehmens aufgedeckt wurden.

Die Zahlen **Italiens** waren höher als die der anderen drei Länder und ergaben sehr große Lücken bei den IT-Abläufen (41 %), bei Visibilität der Bedrohungen der Cybersicherheit (38 %) und bei der Einbindung von Remote-Mitarbeitern (37 %). Die **USA** hatten die höchsten sehr bedeutende Auswirkungen durch Lücken bei der Kommunikation mit Mitarbeitern (30 %), während **Singapur** den höchsten Wert (52 %) bei der Kommunikation mit externen Parteien aufwies. **Italien** und das **Vereinigte Königreich** gaben, gleichauf mit 36 %, die höchsten sehr bedeutenden Lücken bei der Disaster-Recovery-Planung an.

29%
der weltweit Befragten war die größte Bedrohung, keine Mehrfaktor-Authentifizierung einrichten zu können.

Welche der folgenden Bedrohungen in Zusammenhang mit COVID-19 stellten Ihr Unternehmen bisher vor die größte Herausforderung?

Für über ein Viertel der Befragten weltweit (29 %) war das Problem, **keine Multifaktor-Authentifizierung einrichten zu können**, die größte Bedrohung für ihr Unternehmen. An zweiter Stelle lag **Malware im Zusammenhang mit COVID-19** mit 15,5 % sowie an dritter Stelle **das Problem, Software-Patches nicht rechtzeitig bereitstellen zu können** (13 %). 10 % gaben **Phishing** und 6 % **Spear Phishing, IoT-Exposition** und **Probleme im Zuge von Remote Access** an. Andere erwähnenswerte Bedrohungen waren **Masquerading** (4,5 %), **Ransomware** (4 %) und **Social Engineering** (4 %).

Das Problem, **keine Multifaktor-Authentifizierung einrichten zu können**, wurde in **Singapur** und den **USA** mit 32 % als am kritischsten eingeordnet. **Malware im Zusammenhang mit COVID-19** war in **Italien** (21 %) das größte Problem, gefolgt vom **Vereinigten Königreich** (20 %). **Phishing**-E-Mails wurden in **Singapur** als am gefährlichsten eingestuft (12 %).

Multifaktor-Authentifizierung nicht einrichten zu können, war die größte Bedrohung für Unternehmen im Bereich der **Finanzdienstleistungen**. Das gaben 50 % der Befragten aus diesem Bereich an. **Malware im Zusammenhang mit COVID-19** war für Unternehmen aus dem Bereich **Lebensmittel und Getränke** (49 %) und **Professional Services** (30 %) eine große Bedrohung. **Medien und Entertainment** waren am anfälligsten für **Phishing**-E-Mails (29 %).

Malware im Zusammenhang mit COVID-19 war vor allem für kleine Unternehmen ein Problem, speziell solche mit 50 – 250 Mitarbeitern (43 %). Für Unternehmensgrößen von 251 – 500 war die größte Bedrohung, **Multifaktor-Authentifizierung nicht einrichten zu können** (46 %).

Wie und in welchem Maße haben sich Bedrohungen während der Pandemie verändert?

92%
Der höchste Threat Change Increase während der Pandemie war bei mit COVID-19 zusammenhängender Malware zu verzeichnen (92 %).

Der höchste Threat Change Increase während der Pandemie war mit COVID-19 zusammenhängender Malware zu verzeichnen. Hier lag der Threat Change Increase bei 92 %. 53 % dieser Zunahme entfielen auf die Kategorien 51 bis über 100 %. An zweiter Stelle stand **IoT-Exposure** mit einem Threat Change Increase von 89 %, von dem 21 % in die Kategorien 51 bis über 100 % fielen. An dritter Stelle standen **Phishing-E-Mails** mit 89 %, von denen 24,5 % in die Kategorien 51 bis über 100 % fielen. Auch **Spear Phishing** war mit einem Threat Change Increase von 88 % signifikant hoch, wovon knapp ein Viertel (23 %) auf die Kategorien 51 bis über 100 % entfielen.

Von den vier Ländern wies **Italien** mit 96 % den höchsten Gesamtanstieg von **Malware im Zusammenhang mit COVID-19** auf, wobei in den Kategorien 51 % bis über 100 % ein erstaunlicher Anstieg von 70 % zu verzeichnen war. Kurz dahinter folgte das **Vereinigte Königreich** mit 93 % insgesamt und 54 % in den Kategorien 51 % bis über 100 %.

Vor kurzem wurde eine neue Form von Ransomware, das so genannte Coronavirus, entdeckt, und es gibt einen Aufwärtstrend bei Ransomware. Leider gab es für Angreifer nie einen besseren Zeitpunkt, um mit Hilfe von **Ransomware** zu erpressen. **Ransomware** fiel jedoch geringer aus als andere Kategorien. 67 % der Befragten berichteten, dass diese Art der Bedrohung zugenommen hat.

29 % der Befragten weltweit nannten das Problem, **keine Multifaktor-Authentifizierung einrichten zu können**, die größte Bedrohung für ihr Unternehmen. Bezüglich des Threat Change Increases während der Pandemie war dies relativ hoch, wobei 87 % einen Threat Change Increase angaben. 24 % der Befragten gaben sogar Zunahmen zwischen 51 und über 100 % an.

Vollständige Umfrageergebnisse

Haben Sie in den vergangenen zwölf Monaten eine Zunahme der Cyberangriffe festgestellt? Wenn ja, um wie viel?

70 % der befragten deutschen Sicherheitsexperten gaben an, dass sie in den letzten zwölf Monaten einen Anstieg der Cyberattacken beobachtet haben, wobei das durchschnittliche Angriffsvolumen um 54 % anstieg. Das ist ein deutlicher Rückgang gegenüber der letzten Umfrage im Oktober 2019, bei der 99 % einen Anstieg gemeldet hatten.

Überraschenderweise sagten 26 % der Befragten, dass ihr Unternehmen **nicht von Cyberangriffen betroffen** war.

Professional Services meldeten mit 87 % den höchsten durchschnittlichen Anstieg des Angriffsvolumens, gefolgt von der **Fertigungsbranche** mit 62 %.

Unternehmen mit 501-1000 Beschäftigten waren am stärksten betroffen und meldeten einen durchschnittlichen Anstieg des Angriffsvolumens um 61 %.

Sind Cyberangriffe auf Ihr Unternehmen in den letzten zwölf Monaten ausgereifter oder weniger ausgereift geworden?

Die Zunahme des Angriffsvolumens ist zwar zurückgegangen, die Angriffe sind allerdings wesentlich ausgereifter als bisher. **82 % aller Befragten** gaben an, dass die Angriffe ausgereifter geworden seien (im Vergleich zu 45 % im Oktober 2019), wobei die Hälfte aller Befragten (41 %) angab, dass sie **deutlich** ausgereifter geworden seien.

Die **Nahrungsmittel- und Getränkeindustrie** verzeichnete mit 67 % den größten Zuwachs an ausgereifteren Angriffen. Mit knappem Abstand folgte die **Fertigungsbranche** (65 %), vor dem Sektor der **Finanzdienstleistungen** (57 %).

Auch hier sind es die Unternehmen mit einer Größe von **501 bis 1000 Mitarbeitern**, die den Hauptanteil dieser komplexeren Angriffe erleiden. Zwei Drittel (66 %) der Befragten in dieser Größenordnung gaben an, ausgereiftere Angriffe identifiziert zu haben.

501-1000
Unternehmen mit 501-1000 Beschäftigten waren am stärksten betroffen.

41%
der Befragten gab an, dass die Angriffe deutlich ausgereifter geworden seien.

73% der deutschen Sicherheitsexperten gaben an, dass ihre Organisation im vergangenen Jahr einen Cyberangriff erlitt – eine Verbesserung zu 2019.

Dateilose Angriffe wie Living-off-the-Land, PowerShell- und WMI-Angriffe standen in Deutschland mit einem Fünftel (20 %) aller Angriffe an erster Stelle.

Welche Art von Cyberangriff auf Ihr Unternehmen war in den letzten zwölf Monaten am erfolgreichsten?

Dateilose Angriffe wie Living-off-the-Land, PowerShell- und WMI-Angriffe standen in Deutschland mit einem Fünftel (20 %) aller Angriffe an erster Stelle. Dies deutet auf Cyberangriffe hin, die Netzwerke unbemerkt infiltrieren und laterale Bewegungen ermöglichen sollen. Die Frequenz dateiloser Angriffe stieg seit dem Threat Report vom Oktober 2019 exponentiell an. Damals waren es nur 9 % Angriffe dieser Art, und die überwiegende Mehrheit (74 %) stammte von individueller Malware.

Jetzt belegt **individuelle Malware** den zweiten Platz, mit 12 % der Angriffe. **Google-Drive-Angriffe (Cloud-basierte Angriffe)** folgen auf Rang drei mit 11 %.

Unternehmen aus der **Finanzdienstleistungsbranche** verzeichneten die meisten dateilosen Angriffe (43 %), während **Regierungsorganisationen und Kommunalbehörden** im Durchschnitt mehr Angriffe mit individueller Malware feststellten: 32 % der Angriffe auf diesen Sektor erfolgten mit individueller Malware.

Unternehmen mit **501 – 1000 Mitarbeitern** wurden öfter als der Durchschnitt Opfer von dateilosen Angriffen (43 %).

Wie oft erlitt Ihr Unternehmen in den letzten zwölf Monaten einen Cyberangriff?

73 % der deutschen Sicherheitsexperten gaben an, dass ihre Organisation im vergangenen Jahr einen Cyberangriff erlitt. Im Durchschnitt hatte jedes Unternehmen zwei Sicherheitsverletzungen zu verzeichnen. Dies stellt eine kontinuierliche Verbesserung gegenüber Oktober 2019 dar, als 98 % der Unternehmen Breaches meldeten und die durchschnittliche Zahl der erlittenen Sicherheitsverletzungen bei 2,38 pro Unternehmen lag.

Im Februar 2019 lag die durchschnittliche Zahl der gemeldeten Verstöße bei 4,97. Deutsche Organisationen scheinen also auf dem richtigen Weg zu sein.

Zwei Drittel (67 %) der Unternehmen, die von Datenlecks betroffen waren, waren nur einmal betroffen, aber 8 % hatten fünf oder mehr Verstöße erlitten.

Island Hopping

Der Anteil von Sicherheitsverletzungen durch Island Hopping stieg von 2% im Oktober 2019 auf aktuell 8% an.

25%

Ein Viertel der deutschen Unternehmen verzeichnete Sicherheitsverletzungen die auf Schwachstellen in Prozessen zurückzuführen waren.

64%

der Unternehmen gaben an, dass ihrem Unternehmen ein Image-Schaden aufgrund eines Datenlecks entstand.

Was war die häufigste Ursache der Sicherheitsverletzungen?

Als Achillesferse deutscher Unternehmen gelten **Schwachstellen in Prozessen:** So verzeichnete ein Viertel (25 %) der deutschen Unternehmen Sicherheitsverletzungen, die auf instabile Prozesse zurückzuführen waren. 15 % wurden dabei durch eine **Schwachstelle im Betriebssystem** und 13 % durch eine **Drittanwendung** gehackt. **Veraltete Sicherheitsstrukturen** waren die Ursache für 12 % der Datenlecks, **während Island Hopping** von 2 % im Oktober 2019 auf 8 % der Datenlecks im aktuellen Threat Report anstiegen. In Unternehmen mit **1001-2000 Mitarbeitern** stieg diese Zahl sogar auf 19 %.

Im Vergleich zum Report von Oktober 2019 ging Phishing deutlich zurück. Waren zuvor 78 % der Datenlecks auf Phishing zurückzuführen, lag die Zahl dieses Mal bei nur 5 %.

Schwachstellen in Prozessen stellten das größte Problem für Unternehmen im Bereich der **Finanzdienstleistungen** sowie für Unternehmen der **Lebensmittel- und Getränkebranche** dar. In beiden Sektoren waren sie die Ursache für 46 % der Datenlecks und waren darüber hinaus verantwortlich für 54,5 % der Breaches in Unternehmen mit **501-1000 Beschäftigten.**

Island Hopping war im **Gesundheitswesen** für 14 % der Sicherheitsverletzungen und für 17 % der Datenlecks in der **Medien- und Entertainmentbranche** die Ursache. Bei **Regierungs- und Kommunalbehörden** stellte veraltete Sicherheit den größten Faktor dar. 24 % der Datenlecks wurden darauf zurückgeführt.

Welche Folgen hinsichtlich Image und Finanzen hatten diese Datenlecks für Ihr Unternehmen?

Deutsche Unternehmen spüren die Folgen von Sicherheitsverletzungen für das Image stärker als die finanziellen Auswirkungen. Nur ein Viertel (26 %) der Befragten gab finanzielle Folgen an – eine Zunahme um sechs Prozentpunkte gegenüber den 20 % vom Report im Oktober 2019. 60,5 % gaben keine finanziellen Auswirkungen an.

Die Auswirkungen auf das Image fielen schwerwiegender aus. 64 % gaben an, dass ihrem Unternehmen ein Image-Schaden aufgrund einer Sicherheitsverletzung entstand und ein Drittel (33,5 %) aller Befragten bezeichnete diesen Schaden gar als schwerwiegend. Diese Zahlen bedeuten dennoch einen Rückgang gegenüber dem Report vom Oktober 2019. Damals gaben noch 76 % an, schwere Image-Schäden erlitten zu haben.

Die Auswirkungen auf das Image waren bei Unternehmen in der **Fertigungsbranche** am stärksten, wobei 46 % schwere Image-Schäden meldeten.

Welche Steigerung Ihrer Ausgaben für die Cyberabwehr planen Sie in den nächsten zwölf Monaten?

86 % der Sicherheitsexperten rechnen für das kommende Jahr mit steigenden Budgets für die Cyberabwehr. Das ist ein deutlicher Rückgang gegenüber Oktober 2019, als noch 98 % der Befragten eine Erhöhung der Ausgaben planten. Die durchschnittliche geplante Erhöhung beträgt 30 %, ein Rückgang um 10 % gegenüber dem letzten Report.

Die stärkste durchschnittliche Erhöhung planen **Professional Services** mit 34 %.

Unternehmen mit **501-1000 Mitarbeitern** agieren wie bereits festgestellt in einem vergleichsweise stark bedrohten Umfeld und planen mit 33 % eine überdurchschnittliche Steigerung des Budgets für Cyberabwehr.

86%
der Sicherheitsexperten rechnen für das kommende Jahr mit steigenden Budgets - ein Rückgang.

95%
der befragten deutschen Unternehmen setzen Threat Hunting im Rahmen ihrer Strategie für Cybersicherheit ein.

Konnte Ihr Unternehmen in den letzten zwölf Monaten mithilfe von Threat Hunting seine Cyberabwehr stärken und Cyberangriffe aufdecken, die andernfalls übersehen worden wären?

95 % der befragten deutschen Unternehmen setzen Threat Hunting im Rahmen ihrer Strategie für Cybersicherheit ein. Neun von zehn Unternehmen gaben an, dass Threat Hunting ihre Cyberabwehr in gewissem Umfang gestärkt hat, wobei 40 % der Befragten die Wirkung sogar als **signifikant** einstufen.

85 % fanden Hinweise auf Cyberangriffe, die andernfalls unentdeckt geblieben wären; 47 % stuften die Hinweise als **signifikant** ein.

Threat Hunting erweist sich besonders im Bereich der **Finanzdienstleistungen** als wertvoll, wo 76 % der Befragten **signifikante** Hinweise auf Angriffe fanden.

37,5%
der Befragten sehen das Netzwerk als größtes Risiko.

11,15
Im Durchschnitt werden 11,15 Technologien eingesetzt.

37%
kennen das MITRE ATT&CK® Framework aber planen nicht, es einzusetzen.

Führen Sie in den nächsten sechs bis zwölf Monaten 5G ein und müssen Sie Security-Budgets und -Kontrollen erhöhen, um 5G einzuführen (d.h. tätigen Sie Netto-Neuinvestitionen aufgrund dieses neuen Risikos)?

Eine große Mehrheit (94 %) führt 5G in den nächsten zwölf Monaten ein, wobei 60 % dies in den nächsten sechs Monaten beabsichtigen. Die Meinungen zu den Auswirkungen auf die Sicherheit sind dabei unterschiedlich. 51 % gaben an, sie müssen die Ausgaben für Sicherheit erhöhen, um 5G einzuführen, während 43 % nicht glauben, dass sie mehr investieren müssen.

Bei genauerer Betrachtung scheint es eine Spaltung zwischen öffentlichem und privatem Sektor zu geben:

66 % der Unternehmen aus den Branchen **Lebensmittel und Getränke**, 64 % aus dem Bereich **Professional Services** und 58 % aus der **Finanzdienstleistungsbranche** geben an, dass sie ihre Ausgaben für Sicherheit infolge der 5G-Transformation erhöhen werden.

Im Gegensatz dazu planen 57 % der Unternehmen aus dem **Gesundheitswesen** und 47 % der **Regierungs- und Kommunalbehörden** bei der Einführung von 5G **keine** Erhöhung der Ausgaben für Sicherheit.

Wie viele verschiedene Sicherheitstechnologien haben Sie im Rahmen Ihres Sicherheitsprogramms im Einsatz (d.h. mehrere Konsolen, mehrere Agents, mehrere Tools)?

43 % der Unternehmen nutzen im Rahmen ihres Sicherheitsprogramms zwischen elf und 20 verschiedene Technologien. 33,5 % nutzen zwischen fünf und zehn. Das zeugt von komplexen Managementumgebungen, die mit deutlichem Mehraufwand verbunden sind.

Im Durchschnitt werden 11,15 Technologien eingesetzt. Diese Zahl steigt bei Unternehmen der **Fertigungsbranche** auf 14,49. IT-Teams mit 31 – 40 Personen verwenden im Durchschnitt 12,74 Tools.

Mit den meisten Technologien arbeiten Unternehmen mit 501 - 1000 Mitarbeitern – im Durchschnitt 13,91 – wobei 68 % der Unternehmen dieser Größenordnung zwischen elf und 25 verschiedene Technologien nutzen.

Ist Ihnen das MITRE ATT&CK®-Framework zur Validierung Ihrer Sicherheitslage bekannt und planen Sie, es einzusetzen?

Fast drei Viertel (72 %) der deutschen Sicherheitsexperten kennen das MITRE ATT&CK® Framework, aber über seine Verwendung herrscht Uneinigkeit. 35 % planen, es zur Überprüfung ihrer Sicherheitsmaßnahmen zu verwenden, 37 % dagegen nicht. 28 % kennen das Framework nicht.

Das MITRE ATT&CK®-Framework stößt bei Organisationen des öffentlichen Sektors auf die größte Nachfrage, wobei 47 % der R**egierungs- und Kommunalbehörden** und die Hälfte der Befragten im **Gesundheitswesen** planen, es einzusetzen. Im Gegensatz dazu haben 54 % der Unternehmen in der **Fertigungsbranche,** obwohl ihnen das MITRE ATT&CK®-Framework bekannt ist, nicht vor, es einzusetzen.

Welche der folgenden Kategorien erforderten - wenn überhaupt - in den letzten zwölf Monaten eine Verlagerung, also Erhöhung oder Verringerung, der Investitionen (d.h. Repriorisierung des Budgets)?

Der Bereich, in dem Investitionen am häufigsten neu priorisiert werden mussten, ist der der Netzwerke. Das gaben 53 % der Befragten an. An zweiter Stelle stehen Workloads und Anwendungen (38 %), gefolgt von Mobile Device Management, das bei 28 % der befragten Unternehmen eine Repriorisierung der Investitionen verlangte. Endpoints verlangten bei 17,5 % eine Repriorisierung.

Mehr als drei Viertel (76 %) der Befragten aus der **Finanzdienstleistungsbranche** hatten ihre Budgets für Netzwerke neu priorisiert, während Workloads und Anwendungen v.a. für **Gesundheitsorganisationen** ein Thema waren (53 %).

Welcher der folgenden Punkte stellt - wenn überhaupt - das größte Risiko in Ihrem Sicherheitsprogramm dar?

37,5 % der Befragten sehen das Netzwerk als größtes Risiko, gefolgt von Workloads und Anwendungen, die 18 % der Befragten zufolge ein Risiko darstellen. Das am dritthäufigsten genannte Risiko sind Endpoints (17 %) – worunter z.B. Laptops und Desktops fallen.

Ein überdurchschnittlich hohes Risiko im Bereich Netzwerk sehen Unternehmen aus der **Finanzdienstleistungsbranche** (67 %), sowie aus den Branchen **Nahrungsmittel und Getränke** (53 %).

Größere IT-Teams sorgen sich mehr über Workloads und Anwendungen im Allgemeinen als über das Netzwerk oder andere Formen von Risiken für Datenschutzverletzungen.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com