Carbon Black.

GLOBAL THREAT REPORT SERIES

Bedrohungsbericht für Deutschland

Diese Befragungsstudie wurde durchgeführt, um die Herausforderungen zu verstehen, mit denen deutsche Unternehmen derzeit in ihrem Kampf gegen Cyberkriminalität konfrontiert sind. Sie identifiziert Trends beim Hacking sowie bei böswilligen Angriffen und untersucht, wie Unternehmen in Deutschland das Threat Hunting, also die Jagd auf Bedrohungen, einsetzen, um ihre Verteidigungsmaßnahmen zu optimieren.

FEBRUAR 2019

Umfragemethodik

Carbon Black beauftragte im Januar 2019 das unabhängige Marktforschungsunternehmen Opinion Matters mit der Durchführung einer Umfrage. Dabei wurden mehr als 250 CIOs, CTOs und CISOs von deutschen Unternehmen verschiedener Branchen befragt: Finanzdienstleistungen, Gesundheitswesen, Behörden, Einzelhandel, Lebensmittel, Öl und Gas, Professional Services sowie Medien und Unterhaltung. Die Studie ist Bestandteil eines globalen Marktforschungsprojekts, das mehrere Länder abdeckt, darunter Australien, Deutschland, Frankreich, Großbritannien, Italien, Japan, Kanada und Singapur.

Vorwort

DIE CYBERANGRIFFSLANDSCHAFT IN DEUTSCHLAND 2019

Rick McElroy
Leiter für Sicherheitsstrategie, Carbon Black

Wenn Sie ein Unternehmen in Deutschland betreiben, lässt der Report vermuten, dass Sie vermutlich auch Sie zu den erstaunlichen **92%** der befragten Unternehmen gehören, die in den letzten zwölf Monaten einem Cyberangriff zum Opfer gefallen sind. Unsere Recherchen haben ergeben, dass dies vermutlich sogar mehrmals der Fall war, denn Cyberkriminelle greifen immer häufiger mit immer ausgereifteren Methoden an.

Unser erster Bedrohungsbericht für Deutschland beleuchtet die Aggressivität, denen deutsche Unternehmen ausgesetzt sind, und weist darauf hin, dass in der heutigen digitalen Landschaft Verletzungen der Datensicherheit fast unvermeidbar sind. **85%** der befragten Unternehmen in Deutschland meldeten einen Anstieg bei den Cyberangriffen – und **42%** verzeichneten eine Zunahme der Häufigkeit von Angriffen um über **51%**. Zwar sind Unternehmen jeder Größe betroffen, jedoch ist die Bedrohung bei größeren Unternehmen deutlich ernster.

Diese Eskalation in der deutschen Bedrohungslandschaft spiegelt die Ergebnisse des globalen Bedrohungsberichts 2019 von Carbon Black wider,

92% DER BEFRAGTEN UNTERNEHMEN .

in dem Angriffsdaten von insgesamt 15 Millionen von Carbon Black geschützten Endpunkten weltweit ausgewertet wurden. Die Daten belegten für jeden Endpunkt im Durchschnitt zwei Angriffsversuche pro Monat. In einem Unternehmen mit 10.000 Endpunkten finden also pro Tag etwa 660 Cyberangriffe statt.

Angreifer profitieren nach wie vor von erheblichen Ressourcen und Finanzmitteln, und sie nutzen diese größtmöglich zum eigenen Vorteil aus. Sie gehen beim Infiltrieren von Unternehmen langfristig und strategisch durchdacht vor, und bei mehr als **50%** der Angriffe spielen sekundäres Command-and-Control, erneute Angriffe bei Verteidigungsmaßnahmen und Island Hopping eine Rolle*.

Angesichts dieses unerbittlichen Bombardements ist es nicht mehr realistisch, auf eine rein reaktive Verteidigungsstrategie zu setzen. Die Unumgänglichkeit von Sicherheitsverletzungen setzt Unternehmen unter Druck, Angriffsvektoren proaktiv zu erkennen und zu neutralisieren. Dazu ist es erforderlich, die Transparenz zu verbessern, Bedrohungen ausfindig zu machen und effektive Verteidigungsmaßnahmen zu entwickeln.

Immerhin zeigt unsere Studie, dass in Unternehmen das Threat Hunting Fahrt aufnimmt. In Deutschland gilt dies für Unternehmen in allen Branchen, und bei ausgereiften Bereitstellungen zeigen sich durchaus positive Auswirkungen. **92%** der Befragten, die aktiv Threat Hunting betreiben, stellten eine Stabilisierung der Verteidigungsmaßnahmen fest.

Die Größe der Herausforderung für Sicherheitsteams ruft verstärkt auch die Budgetverantwortlichen auf den Plan, da Unternehmen in allen Branchen mit einem Anstieg der Ausgaben für die Cyberabwehr rechnen. Laut unserer Studie planen deutsche Unternehmen eine Vergrößerung der entsprechenden Haushaltsposten um durchschnittlich 26 Prozent.

Dies könnte auf ein Umdenken in Bezug auf das Sicherheitsbudget hinweisen, denn Unternehmen beurteilen die Dimension der ihnen bevorstehenden Herausforderung zunehmend realistisch. Wir glauben, dass dieser Richtungswechsel dringend erforderlich ist, damit Unternehmen die Risiken, die sich heute durch internetbasierte Betriebsabläufe ergeben, effektiv managen können.

Eine sinnvolle Zuteilung des Cyberabwehr-Budgets ist nur möglich, wenn der Ursprung der häufigsten und gefährlichsten Bedrohungen bekannt ist. Wie groß sind die Auswirkungen von Ransomware? Wie entwickeln sich Lieferkettenrisiken? Wir haben Unternehmen gebeten, die häufigsten und schädlichsten Angriffsmethoden zu nennen, um daraus ein detailliertes Gesamtbild der Bedrohungslandschaft als Grundlage für Investitionsempfehlungen und Strategieentscheidungen zu erstellen.

WIR HOFFEN, DASS DIESER ERSTE BEDROHUNGSBERICHT FÜR DEUTSCHLAND FÜR SIE NÜTZLICH UND INFORMATIV IST.

** Laut dem jüngsten Quartalsbericht von Carbon Black zu Cyberbedrohungen (November 2018) https://www.carbonblack.com/quarterly-incident-response-threat-report/november-2018/*

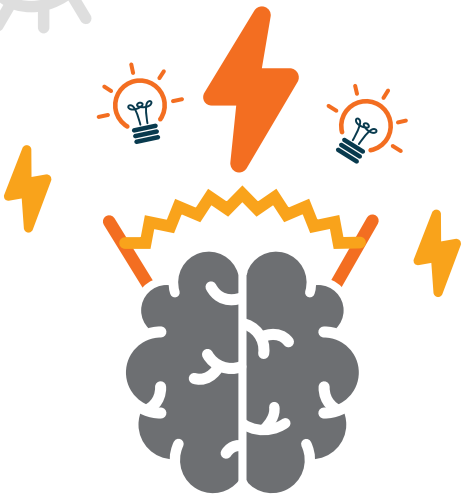
92%

DER BEFRAGTEN UNTERNEHMEN IN DEUTSCHLAND

WICHTIGSTE ERGEBNISSE DER STUDIE

85%

DER UNTERNEHMEN IN DEUTSCHLAND STELLTEN EINE ZUNAHME DER CYBERANGRIFFE IN DEN VERGANGENEN ZWÖLF MONATEN FEST.



72%

GEBEN AN, DASS ANGRIFFE IMMER AUSGEREIFTER WERDEN.

HÄUFIGKEIT VON SICHERHEITSVERLETZUNGEN

92% der befragten Unternehmen in Deutschland gaben an, in den letzten zwölf Monaten Opfer von Sicherheitsverletzungen geworden zu sein, wobei fast die Hälfte (**43%**) von drei bis fünf Vorfällen sprach. Bei **6%** waren es sogar zehn oder mehr Sicherheitsverletzungen. Über alle Branchen hinweg kam es im Durchschnitt zu 4,97 Zwischenfällen.

ESKALIERENDE ANGRIFFE

85% der Unternehmen in Deutschland stellten eine Zunahme der Cyberangriffe in den vergangenen zwölf Monaten fest. Davon gaben **20,5%** einen Anstieg von bis zu **25%** an, bei **22%** waren es zwischen 26 und **50%** und bei **42%** mehr als **50%**.

Der globale Trend zu immer ausgereifteren Angriffen wird in Deutschland dadurch belegt, dass **72%** der Umfrageteilnehmer von einer wachsenden Komplexität der Bedrohungen berichten. **25%** gaben sogar an, dass Angriffe deutlich ausgereifter geworden sind.

MANGELHAFTE KENNTNIS DES UMFANGS DER BEDROHUNGSLANDSCHAFT

Auf die Frage, welchen wirtschaftlichen Umfang die Cyberkriminalität im Dark Web hat, konnten nur **15%** der Unternehmen in Deutschland die richtige Zahl nennen: 1 Billion US-Dollar.

CYBERABWEHR-AUSGABEN IN DEUTSCHLAND

Deutsche Unternehmen planen eine Erhöhung der Cyberabwehr-Ausgaben um durchschnittlich 26 Prozent. Etwas weniger als die Hälfte (**47,5%**) der Unternehmen in Deutschland gab an, ihre Ausgaben um 11 bis **30%** steigern zu wollen.

WELCHE ANGRIFFE RICHTEN MEHR SCHADEN AN?

31% der Datensicherheitsverletzungen gingen auf Phishing-Angriffe oder Ransomware zurück. **25%** waren die Folge von unzureichenden Sicherheitsprozessen oder veralteter Sicherheitssoftware, und bei **13%** waren Schwachstellen im Betriebssystem die Ursache. In Deutschland erfolgten **10%** der

Sicherheitsverletzungen über die Lieferkette, während sich **9%** auf Anwendungen von Drittanbietern zurückführen ließen.

Eine detaillierte Untersuchung, welche Arten von Angriffen am erfolgreichsten waren, hatte folgendes Ergebnis: Standard-Malware (**16,5%**), Ransomware (**16%**) und böswillige Angriffe (**13%**).

Auf die Frage, welche Art von Cyberkriminalität ihrer Meinung nach am effektivsten und schädlichsten sei, führten **29%** sogenannte „Watering Hole"-Angriffe an, bei denen Besucher einer manipulierten Website mit Malware infiziert werden. **22%** nannten das Island Hopping.

THREAT HUNTING NIMMT FAHRT AUF

Auf die Frage, ob sie bereits Threat-Hunting-Methoden eingesetzt haben, um ihre Abwehrmaßnahmen zu stärken, antworteten **35%** der Befragten, dass sie bereits seit über einem Jahr Threat Hunting betreiben, während **37%** erst vor weniger als einem Jahr damit begonnen haben. Von den Umfrageteilnehmern, die aktives Threat Hunting betreiben, sind 92 % der Meinung, dass es ihre Abwehr robuster gemacht hat.

92%
SIND DER MEINUNG, DASS ES IHRE ABWEHR ROBUSTER GEMACHT HAT.

VOLLSTÄNDIGE UMFRAGEERGEBNISSE

WIE OFT IST IHR UNTERNEHMEN IN DEN LETZTEN ZWÖLF MONATEN EINEM CYBERANGRIFF ZUM OPFER GEFALLEN?

92% der befragten Unternehmen in Deutschland gaben an, in den letzten zwölf Monaten Opfer von Sicherheitsverletzungen geworden zu sein, wobei fast die Hälfte (**43%**) von drei bis fünf Vorfällen sprach. Bei **6%** waren es zehn oder mehr Sicherheitsverletzungen.

Sowohl bei Regierungs- und Kommunalbehörden als auch bei Versorgungsunternehmen kam es mit **17%** bzw. **35%** am häufigsten zu mehr als zehn Sicherheitsverletzungen pro Jahr.

Im Privatsektor waren Finanzdienstleister sowie Fertigungs- und Technikunternehmen am stärksten betroffen. In der Finanzdienstleistungsbranche fielen **100%** der Unternehmen

4.97
DURCHSCHNITTLICHE ANZAHL VON SICHERHEITSVERLETZUNGEN IN DEUTSCHEN UNTERNEHMEN PRO JAHR

85%

DER BEFRAGTEN UNTERNEHMEN STELLTEN EINE ZUNAHME DER CYBERANGRIFFE GEGEN IHR UNTERNEHMEN IN DEN VERGANGENEN ZWÖLF MONATEN FEST.

durchschnittlich 5,47 Sicherheitsverletzungen pro Jahr zum Opfer. Bei den Fertigungs- und Technikunternehmen waren es **88%** der Unternehmen mit durchschnittlich 5,7 Sicherheitsverletzungen pro Jahr.

Größere Unternehmen werden häufiger angegriffen. So stellten Unternehmen mit mehr als 20.000 Mitarbeitern im Durchschnitt 6,62 Sicherheitsverletzungen pro Jahr fest.

HABEN SIE IN DEN VERGANGENEN ZWÖLF MONATEN EINE ZUNAHME DER CYBERANGRIFFE FESTGESTELLT? WENN JA, UM WIE VIEL?

85% der befragten Unternehmen stellten eine Zunahme der Cyberangriffe gegen ihr Unternehmen in den vergangenen zwölf Monaten fest.

93% der befragten Finanzdienstleister verzeichneten mehr Cyberangriffe, während Fertigungs- und Technikunternehmen mit **79,6%** einen Rückgang meldeten.

In allen Branchen ist die Anzahl von Angriffen bei größeren Unternehmen stärker angestiegen.

72%

DER BEFRAGTEN GABEN AN, DASS CYBERANGRIFFE GEGEN IHR UNTERNEHMEN IN DEN LETZTEN ZWÖLF MONATEN AUSGEREIFTER GEWORDEN SIND.

SIND CYBERANGRIFFE AUF IHR UNTERNEHMEN IN DEN LETZTEN ZWÖLF MONATEN AUSGEREIFTER ODER WENIGER AUSGEREIFT GEWORDEN?

Der Umfrage zur Folge ist in den Branchen Einzelhandel, Reise und Verkehr sowie Versorgungswirtschaft dieser Trend besonders stark ausgeprägt: Hier waren 33 % bzw. 35 % der Angriffe deutlich ausgereifter als zuvor.

54 % der befragten Unternehmen mit 5.001–10.000 Mitarbeitern, die in den vergangenen zwölf Monaten angegriffen wurden, gaben an, dass Angriffe deutlich ausgereifter geworden sind, während dies nur bei 9 % der Unternehmen mit weniger als 500 Mitarbeitern der Fall ist.

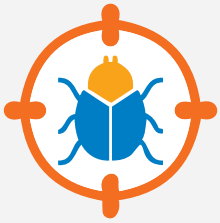
WELCHE ART VON CYBERANGRIFF AUF IHR UNTERNEHMEN WAR IN DEN LETZTEN ZWÖLF MONATEN AM ERFOLGREICHSTEN?

Die Liste wird angeführt von Standard-Malware, Ransomware und böswilligen Angriffen, die gemeinsam **45%** ausmachen.

Finanzdienstleister stellten als häufigsten Angriffstyp böswillige Angriffe fest (**28%**), und bei Fertigungs- und Technikunternehmen fiel die Anzahl von Malware-Angriffen am höchsten aus (**33%**).

Sicherheitsverletzungen über die Lieferkette kamen bei Regierungs- und Kommunalbehörden mit **17%** relativ häufig vor.

Der Einzelhandel vermeldete die höchste Anzahl von Ransomware-Angriffen.



STANDARD-MALWARE RANSOMWARE UND BÖSWILLIGEN ANGRIFFEN

45%

WAS WAR DIE HÄUFIGSTE URSACHE VON ERFOLGREICHEN ANGRIFFEN?

Laut der Studie waren Phishing-Angriffe mit **17%** am häufigsten bei den untersuchten Ergebnissen erfolgreich. Es folgten Ransomware-Angriffe mit **14,5%** und an dritter Stelle veraltete Sicherheitstechnologie und Schwachstellen in Betriebssystemen mit jeweils **13%**, dicht gefolgt von veralteten Prozessen (**12%**) sowie Webanwendungsangriffen und Sicherheitsverletzungen in der Lieferkette (jeweils **10%**).

Mit **40%** hatten Phishing-Angriffe im Bereich Professional Services den höchsten Wert, während es bei den Finanzdienstleistern Ransomware mit **18%** war. Im Gesundheitswesen wurde mit **32%** veraltete Sicherheitstechnologie am häufigsten genannt.

Die Hauptursache für Sicherheitsverletzungen bei Regierungs- und Kommunalbehörden waren, dem Bericht zur Folge, Schwachstellen in Betriebssystemen, bei Fertigungs- und Technikunternehmen waren es Sicherheitsverletzungen über die Lieferkette.

Unternehmen mit 20.001–50.000 Mitarbeitern fielen mit **29%** am häufigsten Phishing-Angriffen zum Opfer.

Unternehmen mit 50–250 Mitarbeitern waren dagegen vor allem von Schwachstellen bei Betriebssystemen betroffen (**28%**).

DER EINZELHANDEL

VERMELDETE DIE HÖCHSTE ANZAHL VON RANSOMWARE-ANGRIFFEN.

PROFESSIONAL SERVICES

40%

MIT 40 % HATTEN PHISHING-ANGRIFFE IM BEREICH PROFESSIONAL SERVICES DEN HÖCHSTEN WERT

90%

DER UNTERSUCHTEN UNTERNEHMEN PLANEN EINE ANHEBUNG IHRES BUDGETS.

IN WELCHER HÖHE PLANEN SIE IHRE AUSGABEN FÜR DIE CYBERABWEHR IN DEN NÄCHSTEN ZWÖLF MONATEN ANZUHEBEN?

90% der untersuchten Unternehmen planen eine Anhebung ihres Budgets.

Bei **26%** sollen die Ausgaben um **11–20%** gesteigert werden.

21% beabsichtigen eine Steigerung um **21–30%, 26%** nennen eine Anhebung um **31–40%**, und bei **14%** sind es **41–50%**. Unternehmen in den Bereichen Reise und Verkehr sowie Gesundheitswesen wollen ihre Ausgaben um mehr als **30%** steigern.

40% der befragten Finanzdienstleister und **50%** der Gesundheitsorganisationen streben **31–40%** höhere Ausgaben an.

Bei größeren Unternehmen (mehr als 20.000 Mitarbeiter) sind noch umfangreichere Ausgabensteigerungen vorgesehen.

WELCHEN WIRTSCHAFTLICHEN UMFANG HAT DIE CYBERKRIMINALITÄT IM DARK WEB?

Nur **15%** der Befragten konnten die richtige Zahl nennen: 1 Billion US-Dollar.

WELCHE ART VON CYBERANGRIFF IST IHRER MEINUNG NACH AM EFFEKTIVSTEN UND AM SCHÄDLICHSTEN?

Fast ein Drittel der Befragten nennt „Watering Hole“-Angriffe, bei denen Besucher einer manipulierten Website mit Malware infiziert werden.

Jedes fünfte untersuchte Unternehmen hält das Island Hopping für die schädlichsten Angriffe, während **14%** Wiper- und Integritätsangriffe am meisten fürchten.

Interessanterweise wurden, dem Bericht zur Folge, „Watering Hole“-Angriffe bei Lebensmittelunternehmen am häufigsten genannt (**67%**), in den Bereichen Medien und Unterhaltung sowie Reise und Verkehr führte dagegen das Island Hopping die Liste an.

Für Finanzdienstleister ist das Island Hopping (**32%**) die schädlichste Angriffsmethode.

Unternehmen im Bereich Professional Services und im Gesundheitswesen halten folglich „Watering Hole“-Angriffe mit **47%** bzw. **41%** für am erfolgreichsten.

Grundsätzlich gilt: Je größer das Unternehmen, desto höher wird die Gefahr durch Island Hopping eingeschätzt, da das Partner-Ökosystem umfangreicher ist. Das bedeutet aber nicht, dass das Risiko bei kleineren Unternehmen geringer ist, denn hier sind besonders ihre Hauptkunden von Sicherheitsverletzungen betroffen.

67%

INTERESSANTERWEISE WURDEN, DEM BERICHT ZUR FOLGE, „WATERING HOLE“-ANGRIFFE BEI LEBENSMITTELUNTERNEHMEN AM HÄUFIGSTEN GENANNT

92%

UNTERNEHMEN, DIE THREAT HUNTING EINSETZEN, GABEN AN, DASS DADURCH IHRE CYBERABWEHR VERBESSERT

73%

DER BEFRAGTEN UNTERNEHMEN IN DEUTSCHLAND BETREIBEN AKTIV

THREAT HUNTING

HAT IHR UNTERNEHMEN IN DEN LETZTEN ZWÖLF MONATEN THREAT HUNTING BETRIEBEN?

73% der befragten Unternehmen in Deutschland betreiben aktiv Threat Hunting.

35% der Unternehmen setzen Threat Hunting seit über einem Jahr ein. **37%** geben an, in den vergangenen zwölf Monaten mit Threat Hunting begonnen zu haben.

Die Situation bei Finanzdienstleistern scheint am ausgereiftesten: **60%** der befragten Unternehmen betreiben Threat Hunting seit über einem Jahr.

92% der Unternehmen, die Threat Hunting einsetzen, gaben an, dass dadurch ihre Cyberabwehr verbessert, bei **41%** sogar deutlich verbessert wurde.

ÜBER CARBON BLACK

Carbon Black (NASDAQ: CBLK) ist ein führender Anbieter von hochmodernen cloudbasierten Endpunkt-Sicherheitslösungen. Carbon Black nutzt seine Cloud-Plattform zur Big Data-Analyse – CB Predictive Security Cloud –, um Prävention, Erkennung, Reaktion, Threat Hunting und Managed Services in einer einzigen Plattform mit nur einem Agent und einer zentralen Konsole zu konsolidieren. Dadurch ist es für Unternehmen einfacher, verschiedene Sicherheitskonzepte zusammenzufassen und den Schutz zu verbessern. Als Vorreiter für Cybersicherheit hat Carbon Black bereits mehreren Endpunkt-Sicherheitskategorien den Weg geebnet, darunter Anwendungskontrolle, Endpoint Detection and Response (EDR) und Next-Generation Antivirus (NGAV), die Kunden selbst gegen die fortschrittlichsten Bedrohungen Schutz bieten. Über 4.600 Kunden weltweit, darunter ein Drittel der Fortune-100-Unternehmen, vertrauen Carbon Black die Sicherheit Ihrer Unternehmen an.

Carbon Black.

Carbon Black
The White Building
1st Floor, Reading
Berkshire
RG1 3AR
T: 01189 082374

carbonblack.com