Carbon Black.
GERMAN

GLOBAL THREAT REPORT SERIES

DIE CYBERABWEHR WIRD BESSER

Carbon Black hat diese Umfrage 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 das Vorgehen deutscher Unternehmen beim Ausbau ihrer IT-Sicherheitsmaßnahmen, ihre Zuversicht bezüglich der Abwehr von Angriffen und ihre Bedenken hinsichtlich dem Fachkräftemangel im Bereich IT-Sicherheit werden untersucht.

OKTOBER 2019

Umfragemethodik

Carbon Black beauftragte im August 2019 das unabhängige Marktforschungsunternehmen Opinion Matters mit der Durchführung einer Umfrage. Befragt wurden 256 deutsche CIOs, CTOs und CISOs von Unternehmen in verschiedenen Branchen, wie etwa Finanzdienstleistungen, Gesundheitswesen, Behörden, Einzelhandel, Fertigung, Lebensmittel, Versorgungsbetriebe, Professional Services sowie Medien und Unterhaltung. Der zweite Carbon Black Threat Report für Deutschland baut auf dem ersten Threat Report von Januar 2019 auf. Neben Deutschland werden für den Threat Report auch IT-Führungskräfte aus Australien, Frankreich, Großbritannien, Italien, Japan, Kanada und Singapur befragt.

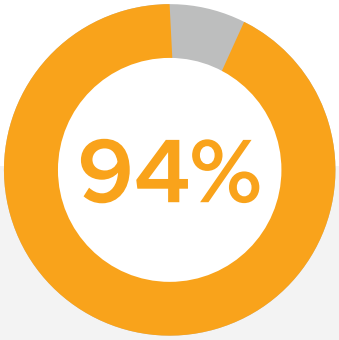
VORWORT

DIE LAGE DER IT-SICHERHEIT IN DEUTSCHLAND 2019

Rick McElroy
Head of Security Strategy, Carbon Black

Deutsche Unternehmen sehen sich mit einer dramatischen Zunahme an Cyberbedrohungen konfrontiert. In den letzten zwölf Monaten ist die Zahl der Cyberangriffe exponentiell gestiegen. Vor allem die in Deutschland starke Fertigungsbranche ist ein attraktives Ziel für Cyberkriminelle: CIOs, CTOs und CISOs aus dieser Branche sagen, dass die Angriffe deutlich zugenommen haben.

Aufgrund der vielfältigen Bedrohungen sind Sicherheitsverletzungen fast schon unvermeidbar geworden. Ein Blick auf die Schlagzeilen zu dem Thema bestätigt die Ergebnisse des zweiten Carbon Black Threat Reports für Deutschland, die sind:



DER BEFRAGTEN UNTERNEHMEN GABEN AN, DASS IHR RUF DURCH DATENSCHUTZVERLETZUNGEN BESCHÄDIGT WURDE.

98% der Unternehmen in Deutschland, die befragt wurden, gaben an, in den letzten zwölf Monaten aufgrund von externen Cyberangriffen eine oder mehrere Datenschutzverletzungen erlitten zu haben.

20% der Unternehmen gaben an, dass diese Sicherheitsverletzungen gemessene negative finanzielle Auswirkungen hatten. Doch 64% der deutschen Unternehmen wollten keine Angaben über negative finanzielle Auswirkungen im Zuge von erlittenen Datenlecks machen. Stark leidet auch das Unternehmensimage unter den Sicherheitsvorfällen:

94% der befragten Unternehmen gaben an, dass der Ruf durch Datenschutzverletzungen beschädigt wurde. 76% stuften den Imageschaden sogar als schwerwiegend ein.

99% der teilnehmenden deutschen Unternehmen stellten eine Zunahme der Cyberangriffe gegen ihr Unternehmen in den vergangenen zwölf Monaten fest. Im Carbon Black Threat Report von Januar 2019 waren es noch 85%. In Bezug auf die Komplexität unterschieden sich die Angriffe je nach Branche: Finanzdienstleister und der öffentliche Sektor sind mit Cyberangriffen steigender Komplexität konfrontiert, Unternehmen aus der Fertigungsbranche berichteten dagegen abnehmende Komplexität.

Die Datenschutzverletzungen aufgrund von Phishing haben so stark zugenommen, dass Phishing jetzt der Angriffstyp ist, der die meisten Sicherheitsverletzungen nach sich zieht. Das könnte darauf zurückzuführen sein, dass sich die Angreifer auf das schwächste Glied in der IT-Sicherheit konzentrieren – den Benutzer.

WACHSENDE ZUVERSICHT IN DIE EIGENEN FÄHIGKEITEN ZUR ABWEHR VON CYBERANGRIFFEN...

Trotz der ständigen Bedrohungen und deren teilweise gravierenden Folgen fühlen sich 95% der Befragten heute zuversichtlicher hinsichtlich ihrer Fähigkeiten zur Abwehr von Cyberangriffen als vor zwölf Monaten. Dies lässt darauf schließen, dass bei den Unternehmen die verfügbaren Tools und Verteidigungsmechanismen für eine robuste Cyberabwehr stärker in den Fokus rücken und die IT-Sicherheitsteams sowie ausgerollte Technologie heute ausgereifter sind.

Immer mehr Unternehmen aus allen Branchen sehen zudem die Vorteile von Investitionen in die Cybersicherheit: 98% planen eine Steigerung ihres Budgets für IT-Sicherheit in den nächsten zwölf Monaten.

... ABER AUCH MEHR BEDENKEN IN BEZUG AUF DIE RISIKEN NEUER TECHNOLOGIEN

Sicherheitsexperten haben erhebliche Bedenken, wie sich Projekte zur digitalen Transformation und die Implementierung von 5G auf das Risikoniveau auswirken werden. 77% der Befragten gehen davon aus, dass im Zuge dessen die Angriffsflächen für Cyberangriffe zunehmen werden.

FACHKRÄFTEMANGEL IST GROSSE SORGE

Angesichts aktueller und neu entstehender Risiken gaben 58% der befragten CIOs an, ein größeres Team für angemessene Reaktionen darauf zu benötigen. Allerdings stellten 89,5% fest, dass Anwerbung und Schulung von Spezialisten für Cybersicherheit heute schwieriger ist als noch vor zwölf Monaten. Der Fachkräftemangel ist schon absehbar und wird deutsche Unternehmen vor erhebliche Probleme stellen, die Herausforderungen für bessere IT-Sicherheit zum Schutz ihrer Organisation zu meistern.

THREAT HUNTING ERREICHT HÖHEREN REIFEGRAD

Threat Hunting löst seine Versprechen ein: 96% der Unternehmen gaben an, dass Threat-Hunting-Aktivitäten ihre Cyberabwehr gestärkt haben. Ebenfalls 96% haben bei Threat-Hunting-Aktivitäten Hinweise auf Cyberangriffe gefunden, die andernfalls übersehen worden wären.

247%

UNTERNEHMEN MIT MEHR ALS 100.000 ANGESTELLTEN MELDETEN EINE DURCHSCHNITTLICHE STEIGERUNG DER CYBERANGRIFFE UM 247%

WICHTIGSTE ERGEBNISSE DER STUDIE

98%

GABEN AN, EINE
DATENSCHUTZVERLETZUNG
ERLITTEN ZU HABEN

HÄUFIGKEIT VON DATENSCHUTZVERLETZUNGEN

98% der befragten deutschen Unternehmen haben in den letzten zwölf Monaten aufgrund von externen Cyberangriffen eine oder mehrere Datenschutzverletzungen erlitten. Im Vergleich zum Carbon Black Threat Report von Januar 2019 ist dies ein Anstieg um 6%. Allerdings ist die durchschnittliche Anzahl von Sicherheitsverletzungen pro Unternehmen von 4,97 (Januar 2019) nun auf 2,38 zurückgegangen. Dies könnte ein Hinweis darauf sein, dass Unternehmen sich darauf konzentrieren, die Häufigkeit von Sicherheitsverletzungen zu reduzieren.

ANZAHL DER CYBERANGRIFFE STEIGT

Ganze 99% der befragten deutschen Unternehmen gaben an, dass Cyberangriffe immer häufiger werden. Das ist eine starke Veränderung, im Januar 2019 vertraten nur 85% diese Ansicht.

Besorgniserregend ist insbesondere die starke Zunahme der Cyberangriffe. Im Durchschnitt über alle Branchen hinweg ist die Angriffsfrequenz um 194% gestiegen. 90% der Befragten aus der Fertigungsbranche gaben sogar an, dass die Zahl der Angriffe zwischen 201-300% zugenommen hat, eine durchschnittliche Zunahme um 231% in dieser Branche. Dieser Trend findet sich auch in der Finanzdienstleistungsbranche (Zunahme der Angriffe um 153%) sowie bei Medien und Unterhaltung (Zunahme der Angriffe um 188%) wieder.

Große Unternehmen sind mit den größten Bedrohungen konfrontiert: Unternehmen mit mehr als 100.000 Angestellten meldeten eine durchschnittliche Steigerung der Cyberangriffe um 247%, während Unternehmen mit 501-1.000 Angestellten eine vergleichsweise geringe Steigerung der Angriffe um 60% meldeten.

70%

DER BEFRAGTEN STELLTEN FEST, DASS DIE KOMPLEXITÄT DER ANGRIFFE ABGENOMMEN HAT

ÄNDERUNGEN BEI DER KOMPLEXITÄT DER CYBERANGRIFFE SIND BRANCHENABHÄNGIG

Insgesamt hat der zweite Carbon Black Threat Report einen Rückgang bei der Komplexität der Angriffe ergeben. Vor allem in der Fertigungsbranche gaben 70% der Befragten an, dass die Komplexität der Angriffe abgenommen hat.

Doch in den meisten anderen Branchen, darunter Behörden auf Staats- und Kommunalebene, Finanzdienstleistung, Gesundheitswesen und Professional Services, sind die Befragten der Meinung, dass die Cyberangriffe ausgefeilter geworden sind.

UNTERNEHMEN GEBEN IMAGEVERLUST DURCH SICHERHEITSVERLETZUNG EHER ZU ALS FINANZIELLE SCHÄDEN

Eines von fünf befragten Unternehmen gab an, dass Sicherheitsverletzungen gemessene negative finanzielle Auswirkungen hatten. Fast zwei Drittel wollten hingegen keine Angaben über negative finanzielle Auswirkungen im Zuge von erlittenen Datenlecks machen.

94% der befragten Unternehmen gaben an, dass der Ruf durch Datenschutzverletzungen beschädigt wurde. 76% stuften den Imageschaden sogar als schwerwiegend ein. Nur in der Fertigungsbranche schätzten sogar 92% den wegen einer Datenschutzverletzung erlittenen Imageschaden als schwerwiegend ein. Bei Unternehmen mit mehr als 100.000 Angestellten sahen ganze 99% die nach einer Datenschutzverletzung auftretende Rufschädigung als schwerwiegend an.

WACHSENDE ZUVERSICHT IN DIE EIGENEN FÄHIGKEITEN ZUR ABWEHR VON CYBERANGRIFFEN

Insgesamt gaben 95% der befragten Unternehmen an, heute mehr Vertrauen in ihre Fähigkeiten zur Abwehr von Cyberangriffen zu haben als vor einem Jahr. Dies lässt darauf schließen, dass sich Unternehmen den Cyberbedrohungen stärker bewusst sind, ihnen aber dank der fortentwickelten IT-Sicherheitsbranche mehr Tools zur Verfügung stehen, um sich effektiv schützen zu können.

BEDENKEN WEGEN DIGITALER TRANSFORMATION UND 5G IMPLEMENTIERUNG

99% der befragten CIOs/CISOs äußerten Bedenken hinsichtlich der Auswirkungen von Projekten zur digitalen Transformation und der Implementierung von 5G auf die Cybersicherheit. Diese reichten von den umfangreicheren Angriffsmöglichkeiten, die sich Cyberkriminellen bieten, bis hin zum Bedarf an spezialisierten Ressourcen. Zudem waren 58% der Unternehmen der Meinung, das gestiegene Risiko nur mit einem größeren Team bewältigen zu können.

ANWERBUNG UND SCHULUNG EIN PROBLEM FÜR GUT NEUN VON ZEHN DEUTSCHEN UNTERNEHMEN

Unternehmen brauchen mehr Mitarbeiter für größere Teams, jedoch wird sich dieser Bedarf kaum erfüllen lassen. 90% der Umfrageteilnehmer beklagten, dass Anwerbung und Schulung von Fachkräften für IT-Sicherheit in den letzten zwölf Monaten schwierig bzw. sehr schwierig (64,5%) geworden ist.

Vollständige Umfrageergebnisse:

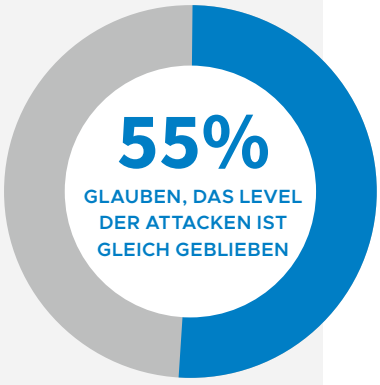
MEHR
ANGRIFFE

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

99% der befragten Unternehmen in Deutschland stellten eine Zunahme der Cyberangriffe auf ihr Unternehmen in den vergangenen zwölf Monaten fest. Dies ist ein deutlicher Anstieg im Vergleich zur Umfrage von Januar 2019, dort lag dieser Wert noch bei 85%.

90% der Unternehmen aus der Fertigungsbranche, 70% der Unternehmen aus der Medien- und Unterhaltungsbranche sowie 47% der Unternehmen der Finanzdienstleistungsbranche gaben an, dass die Häufigkeit der Angriffe um 201-300% gestiegen ist.

Unternehmen mit mehr als 100.000 Angestellten meldeten eine durchschnittliche Steigerung der Cyberangriffe um 247%, der Anstieg der Angriffe ist hier am größten. Dazu passend verzeichneten Unternehmen, deren IT-Abteilungen über 100 Mitarbeiter umfassen, 240% mehr Angriffe.

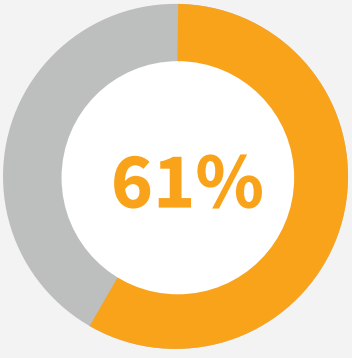


SIND CYBERANGRIFFE AUF IHR UNTERNEHMEN IN DEN LETZTEN ZWÖLF MONATEN AUSGEREIFTER ODER WENIGER AUSGEREIFT GEWORDEN?

Trotz des drastischen Anstiegs bei der Zahl der Angriffe hatte die Mehrheit (55%) der befragten deutschen Unternehmen den Eindruck, die Komplexität der Angriffe sei gleich geblieben oder eher zurückgegangen. Dies ist ein deutlicher Unterschied zum Carbon Black Threat Report von Januar 2019, als 72% die Ansicht vertraten, Angriffe seien ausgereifter geworden.

67% der Unternehmen aus der Fertigungsbranche und 60% der Befragten im Bereich Medien und Unterhaltung waren der Meinung, dass Angriffe etwas weniger ausgereift waren als früher.

Andererseits gaben 61% der Unternehmen aus der Finanzdienstleistungsbranche an, dass die Angriffe ausgereifter geworden sind. Gleiches gilt für 86% der Behörden auf Staats- und Kommunalebene sowie für alle Organisationen aus der Gesundheitsbranche.



DER UNTERNEHMEN AUS DER FINANZDIENSTLEISTUNGSBRANCHE STELLTEN AUSGEREIFTERE ATTACKEN FEST

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

Die Umfrage ergab, dass individuelle Malware mit großem Abstand die in deutschen Unternehmen am häufigsten festgestellte Angriffsart war. 74% der Befragten gaben dies an. Das ist ein drastischer Anstieg im Vergleich zum Threat Report von Januar, in dem nur 16,5% der Teilnehmer Malware als häufigste Angriffsart nannten.

Individuelle Malware stand in den Branchen Finanzdienstleistungen, Fertigung, Medien und Unterhaltung sowie Professional Services an erster Stelle.

Mit 9% standen dateilose Angriffe an zweiter Stelle der häufigsten Angriffsarten.

In der Gesundheitsbranche dagegen traten SSH-Angriffe häufiger als alle anderen Angriffsarten auf, 33% der Unternehmen gaben sie als häufigste Angriffsart an.

UNTERNEHMEN AUS DER FERTIGUNGSBRANCHE

INDIVIDUELL ANGEPASSTE MALWARE

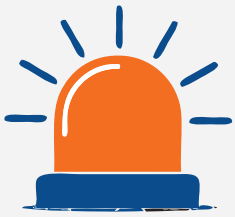
WIE OFT HAT IHR UNTERNEHMEN IN DEN LETZTEN ZWÖLF MONATEN IM ZUGE EINES CYBERANGRIFFS EINE DATENSCHUTZVERLETZUNG ERLITTEN?

Die Mehrheit (77%) der befragten deutschen Unternehmen war in den letzten 12 Monaten nur ein einziges Mal von einem Cyberangriff betroffen, der zu einer Datenschutzverletzung geführt hat. Bei 19% waren es fünf oder mehr Datenschutzverletzungen.

Die durchschnittliche Anzahl von Datenschutzverletzungen, denen deutsche Unternehmen zum Opfer fielen, liegt mit 2,38 Datenschutzverletzungen pro Unternehmen deutlich unter dem im Carbon Black Threat Report von Januar 2019 ermittelten Wert von 4,97.

Im Einzelhandel war die durchschnittliche Zahl von Sicherheitsverletzungen mit 7,8 pro Jahr sehr hoch. Für die Fertigungsbranche ergab sich ein sehr niedriger Wert von nur 1,49. Kleinere Unternehmen erlitten häufiger Datenschutzverletzungen. Unternehmen mit 50-250 Mitarbeitern waren im Durchschnitt von 7,4 Sicherheitsverletzungen pro Jahr betroffen. Große Unternehmen mit mehr als 100.000 Mitarbeitern erlitten durchschnittlich 1,15 Datenschutzverletzungen pro Jahr.

Generell lässt sich festhalten: Je kleiner das IT-Team, desto höher die Anzahl der gemeldeten Datenschutzverletzungen. Unternehmen mit IT-Teams mit weniger als zehn Mitarbeitern verzeichneten durchschnittlich fünf Sicherheitsverletzungen, während Unternehmen mit Teams mit mehr als 100 Mitarbeitern durchschnittlich nur 1,34 pro Jahr feststellten.



MALWARE

BEI **74%**

DIE AM HÄUFIGSTEN FESTGESTELLTE ANGRIFFSART

19%

ERLITTEN FÜNF ODER MEHR DATENSCHUTZVERLETZUNGEN

78%
PHISHING-ANGRIFFE
SIND DIE HAUPTURSACHE VON DATENSCHUTZVERLETZUNGEN

Phishing-Angriffe waren die Hauptursache von Datenschutzverletzungen bei 92% der Unternehmen aus der Fertigungsbranche, bei 69% der Unternehmen aus der Finanzdienstleistungsbranche und bei 82% der Unternehmen aus dem Bereich Professional Services.

94%
GABEN AN, DASS DER RUF DURCH DATENSCHUTZVERLETZUNGEN
BESCHÄDIGT
WURDE

Für 92% der Unternehmen aus der Fertigungs- und für 72% aus der Finanzdienstleistungsbranche war der erlittene Imageschaden schwerwiegend.

WAS WAR DIE HÄUFIGSTE URSACHE DER DATENSCHUTZVERLETZUNGEN?

Phishing ist bei 78% der teilnehmenden deutschen Unternehmen die Hauptursache von Datenschutzverletzungen. Das spiegelt den globalen Trend wider. Auch im Threat Report vom Januar 2019 hatte Phishing die Spitzenposition inne, allerdings wurde es damals nur von 17 % der Umfrageteilnehmer als Hauptursache genannt.

Die zweithäufigste Ursache waren Schwachstellen im Betriebssystem, gefolgt von Ransomware an dritter Stelle.

Sicherheitsverletzungen aufgrund von Prozessstörungen und veralteter Technologie gingen von 25% im Januar 2019 auf nur 5% zurück. Dies lässt darauf schließen, dass Unternehmen Faktoren, die sie selbst beeinflussen können, stärker kontrollieren.

WELCHE FOLGEN HINSICHTLICH IMAGE UND FINANZEN HATTEN DIESE DATENSCHUTZVERLETZUNGEN FÜR IHR UNTERNEHMEN?

20% der deutschen Unternehmen, die von einer Datenschutzverletzung betroffen waren, berichteten von negativen finanziellen Folgen. Dies ist jedoch nicht das ganze Bild. 64% zogen es vor, keine Angaben zu finanziellen Verlusten zu machen.

Diese Zurückhaltung war in der Fertigungsbranche am größten: Hier machten 88% der Betroffenen keine Aussage über die Auswirkungen der Sicherheitsverletzungen. Nur 7% berichteten über negative finanzielle Folgen. Bei Unternehmen mit über 100.000 Mitarbeitern schwiegen sich 93% über eventuelle finanzielle Folgen aus.

Hinsichtlich den Imagefolgen äußerten sich mehr Unternehmen. 94% gaben an, dass ihr Ruf durch Datenschutzverletzungen beschädigt wurde. 76% stuften den Imageschaden sogar als schwerwiegend ein.

WELCHE ANHEBUNG IHRER AUSGABEN FÜR DIE CYBERABWEHR PLANEN SIE IN DEN NÄCHSTEN ZWÖLF MONATEN?

Angesichts der wachsenden Bedrohungen planen 98% der befragten Unternehmen in Deutschland eine Anhebung ihres Budgets für Cyberabwehr im kommenden Jahr. In der Umfrage von Januar 2019 waren es noch neun von zehn Unternehmen.

Die geplanten Budgetsteigerungen sind signifikant. 71% peilen eine Budgetsteigerung zwischen 41 und 50% an. Der Durchschnitt der geplanten Budgetsteigerungen wächst von 26% auf 40%.

Der Trend wird von der Fertigungsbranche angeführt, wo Budgetsteigerungen um durchschnittlich 44% geplant sind, gefolgt von Medien und Unterhaltung sowie Lebensmittel mit einer geplanten Steigerung von jeweils gut 40%.

Die Zahlen legen nahe, dass größere Unternehmen größere Budgetsteigerungen planen. 99% der befragten Unternehmen mit mehr als 100.000 Mitarbeitern planen eine Steigerung um 41-50%.

98%
PLANEN EINE
STEIGERUNG
IHRES BUDGETS FÜR IT-SICHERHEIT

KONNTE IHR UNTERNEHMEN IN DEN LETZTEN ZWÖLF MONATEN MITHILFE VON THREAT HUNTING SEINE CYBERABWEHR STÄRKEN UND CYBERANGRIFFE AUFDECKEN, DIE ANDERNFALLS ÜBERSEHEN WORDEN WÄREN?

Deutsche Unternehmen profitieren von Threat Hunting. 96% der Teilnehmer gaben an, dass Threat Hunting ihre Cyberabwehr in gewissem Umfang gestärkt hat. 78,5% stellten sogar einen signifikanten Sicherheitsgewinn fest. Dies ist eine Steigerung von 37,5% im Vergleich zur Umfrage von Januar 2019. Dort gaben erst 41% der Befragten an, dass ihre Abwehr durch Threat Hunting signifikant gestärkt wurde.

85,5% der Befragten deckten dank Threat Hunting eindeutige Hinweise auf Cyberangriffe auf. Bei Unternehmen aus der Branche Medien und Unterhaltung waren es 90% und bei denen aus der Fertigungsbranche sogar 95%.

96%
THREAT HUNTING HAT
CYBERABWEHR
GESTÄRKT

WAS SIND DIE GRÖSSTEN IT-SICHERHEITSBEDENKEN IHRES UNTERNEHMENS HINSICHTLICH DER IMPLEMENTIERUNG UND MANAGEMENT VON PROGRAMMEN ZUR DIGITALEN TRANSFORMATION UND/ODER 5G?

Die von deutschen Umfrageteilnehmern am häufigsten genannte Sorge war, dass sich dadurch mehr Möglichkeiten für Cyberangriffe ergeben (77%). An zweiter Stelle lag die Notwendigkeit eines größeren Teams (58%), gefolgt vom Bedarf nach stärker spezialisierten Ressourcen (55%).

Befragte der Branche Professional Services haben andere Bedenken. Sie befürchten, dass digitale Transformation und 5G der Cyberkriminalität effektivere und destruktivere Methoden eröffnen

werden. Diese Befürchtung steht auch bei Unternehmen aus der Finanzdienstleistungsbranche recht weit oben, nämlich an zweiter Stelle. Unternehmen der Medien- und Unterhaltungsbranche machen sich dagegen vor allem über die mangelnde Transparenz aufgrund dieser Entwicklungen Gedanken.

WIE ZUVERSICHTLICH IST IHR UNTERNEHMEN IN BEZUG AUF SEINE FÄHIGKEITEN, CYBERANGRIFFE UND SICHERHEITSVERLETZUNGEN ABZUWEHREN IM VERGLEICH ZU VOR 12 MONATEN?

Eine deutliche Mehrheit (95%) der befragten deutschen CIOs haben mehr Vertrauen in ihre Fähigkeit, sich gegen Cyberangriffe zur Wehr zu setzen als vor zwölf Monaten. 68% haben wesentlich mehr Vertrauen.

Unternehmen aus der Finanzdienstleistungs-, Fertigungs- sowie Medien- und Unterhaltungsbranche sind insgesamt am zuversichtlichsten. Aus diesen Branchen gaben über 69% an, wesentlich mehr Vertrauen zu haben.

WIE HABEN SICH ANWERBUNG UND SCHULUNG VON AUF CYBERABWEHR SPEZIALISIERTEM IT-PERSONAL ÜBER DIE LETZTEN ZWÖLF MONATE ENTWICKELT?

89,5% der befragten Unternehmen in Deutschland beurteilen Anwerbung und Schulung von IT-Sicherheitsexperten heute als schwieriger. In den größten befragten Unternehmen (über 100.000 Mitarbeitern) ist die Lage sogar noch ernster: 96% bezeichneten die Anwerbung benötigter Fachkräfte als deutlich schwieriger als vor zwölf Monaten.

Die Fertigungsbranche spürt den Druck auch: 78% Unternehmen aus dieser Branche gaben an, dass Anwerbung und Schulung im August 2019 deutlich schwieriger waren. Aber auch Unternehmen aus der Finanzdienstleistungsbranche haben es nicht leicht. 58% von ihnen beklagen deutlich größere Schwierigkeiten dabei, die benötigten Fachkräfte zu finden.

89,5%
BEURTEILEN RECRUITING ALS
VIEL SCHWIERIGER

ZITATE

Rick McElroy

Head of Security Strategy, Carbon Black

Die Ergebnisse unseres zweiten Carbon Black Threat Reports für Deutschland lassen sich mit dem ersten Carbon Black Threat Report vom Januar 2019 vergleichen. Damit ergibt sich ein klareres Bild der Bedrohungen, mit denen deutsche Unternehmen konfrontiert sind, und wie sie mit diesen Bedrohungen umgehen.

Unternehmen scheinen sich auf die neue Realität kontinuierlicher Cyberangriffe einzustellen. Datenlecks haben große finanzielle Auswirkungen und schädigen die Reputation immens, was immer mehr Unternehmen bewusst wird. Die gestiegene Awareness gegenüber externen Bedrohungen und Compliance-Risiken sorgt dafür, dass Unternehmen Cyberrisiken deutlich proaktiver als früher adressieren.

Wir haben festgestellt, dass Unternehmen Faktoren, die sie selbst beeinflussen können, stärker kontrollieren. Dazu gehören etwa Schwachstellen in Prozessen und veraltete Lösungen für IT-Sicherheit. So verbessern sie schrittweise ihre Sicherheitskonzepte von innen heraus. Gleichwohl ist Phishing nach wie vor die Hauptursache der meisten Datenschutzverletzungen. Das zeigt, dass Unternehmen noch viel Arbeit vor sich haben, ihre Mitarbeiter einzubeziehen und gegenüber Phishing und Social Engineering zu sensibilisieren.

Threat Hunting lohnt sich: Teams decken Bedrohungen auf, die ohne Threat-Hunting-Lösungen übersehen worden wären. Wir sind überzeugt, dass das aktive Vorgehen gegen Angreifer zweifellos zur größeren Zuversicht der Unternehmen beiträgt, heute besser für die Abwehr von Cyberangriffen gerüstet zu sein als vor zwölf Monaten. In Kombination mit den zunehmenden Budgetsteigerungen für IT-Sicherheit ist dies ein gutes Zeichen dafür, dass die Cybersicherheit immer ausgereifter wird und Unternehmen sie effektiv priorisieren.

Zwar wächst die Zuversicht, jedoch räumen CIOs auch Bedenken in Bezug auf geschäftskritische Projekte ein, wie etwa die digitale Transformation und die Einführung von 5G-Netzen. Die Angriffsfläche wird größer und die Abhängigkeit von digitalen Strukturen steigt, dadurch wächst das Risiko von Angriffen. Deutsche Unternehmen fürchten zusätzliche Möglichkeiten für Cyberkriminalität sowie den Einsatz von effektiveren und destruktiveren Angriffsmethoden.

Es besteht die Befürchtung, dass sich diese neuen Bedrohungen nur mit größeren Sicherheitsteams bekämpfen lassen. Doch neue Experten anzuwerben, ist wegen des Fachkräftemangels und des hohen Konkurrenzdrucks eine große Herausforderung. Die Lücke zwischen der benötigten Anzahl von Mitarbeitern mit dem entsprechenden Kompetenzniveau und den auf dem Arbeitsmarkt verfügbaren Experten wird immer größer.

Daher sind Unternehmen gezwungen, ihre IT-Sicherheit mit großer Kreativität und Sorgfalt zu adressieren. Eine höhere Automatisierung, KI und Tools, die selbst in komplexen und ständig wachsenden Netzwerken für umfassende Transparenz sorgen, werden unverzichtbar sein. Ressourceneffizienz wird immer mehr zum Schlagwort: Unternehmen müssen einerseits die Fähigkeit ihrer Teams maximieren, Bedrohungen zu erkennen und abzuwehren, andererseits aber auch intelligent in Tools investieren, die es den Teams ermöglichen, auf der wachsenden Zuversicht aufzubauen und eine proaktive Cyberabwehr beizubehalten.

Wir hoffen, dass der zweite Carbon Black Threat Report für Deutschland für Sie wertvoll und informativ war. Auf Twitter können Sie unter @infosecrick gerne direkten Kontakt mit mir aufnehmen.

@infosecrick

ÜBER CARBON BLACK

Carbon Black (NASDAQ: CBLK) ist ein führender Anbieter von Cloud-nativen Lösungen für den Schutz von Endpoints. Die Mission von Carbon Black ist der weltweite Schutz vor Cyberangriffen. Die CB Predictive Security Cloud® (PSC) vereint den Schutz von Endpoints und IT Operations in einer Endpoint Protection Platform (EPP) zur Abwehr von komplexen Bedrohungen und Bereitstellung von verwertbaren Erkenntnissen. Die PSC ermöglicht Unternehmen jeder Größe, Betriebsabläufe zu vereinfachen. Durch die Analyse von Milliarden von Security Events weltweit pro Tag gewinnt Carbon Black Einblicke in das Verhalten von Angreifern und versetzt seine Kunden in die Lage, potenzielle Angriffe zu erkennen, zu verhindern und darauf zu reagieren.

Über 5.600 Kunden weltweit, darunter ein Drittel der Fortune 100, vertrauen Carbon Black, um ihr Unternehmen vor Cyberangriffen zu schützen. Das Partnernetzwerk des Unternehmens umfasst mehr als 500 MSSPs, VARs, Distributoren und Technologieintegratoren sowie einige der weltweit führenden IR-Unternehmen, die Lösungen von Carbon Black bei der Untersuchung von jährlich über 500 Sicherheitsverletzungen einsetzen.

Carbon Black, CB ThreatSight and CB Predictive Security Cloud are registered trademarks or trademarks of Carbon Black, Inc. in the United States and/or other jurisdictions.

Carbon Black.

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

carbonblack.com