CARBONITE an opentext company | WEBROOT an opentext company

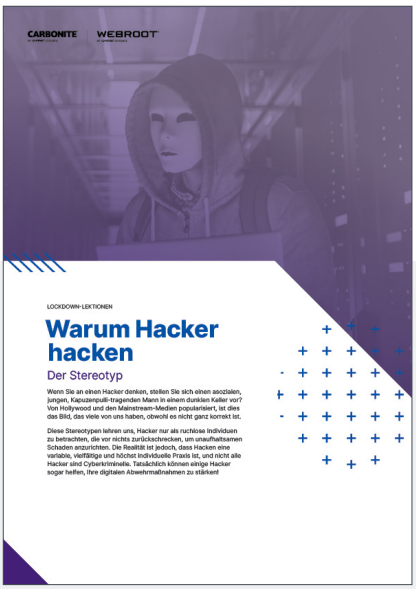
LOCKDOWN-LEKTIONEN

Warum Hacker hacken

Einführung

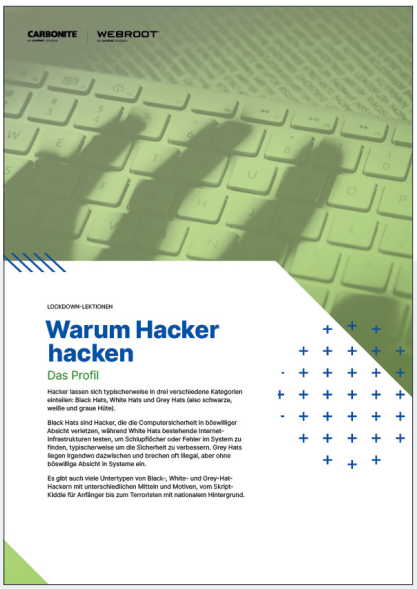
Da die Cybersicherheit immer komplexer wird, entwickeln sich auch die kriminellen Methoden auf der ganzen Welt mit ihr weiter. Die Methoden Krimineller machen Sie angreifbar und viele Unternehmen sind gefährdet. Es ist wichtig, über diese sich ständig verändernde Landschaft informiert zu bleiben. In diesem lehrreichen eBook untersuchen wir, wie Hacker denken, und geben einen Einblick in ihre Welt. Erfahren Sie, warum es wichtig ist, die gängigen Klischees zu entlarven, sich über ihre Methoden und Motive zu informieren und herauszufinden, auf wen sie am meisten abzielen. Die IT-Sicherheitsexperten Tyler Moffitt, Kelvin Murray und Grayson Milbourne helfen Ihnen, sich in den unsicheren Gewässern von heute zurechtzufinden, und geben Tipps, wie Sie Ihr Unternehmen absichern und Ihre Kunden vor laufenden Bedrohungen schützen können.

Es ist Ihre Aufgabe, sich darum zu kümmern!
Webroot.com/LockdownLessons



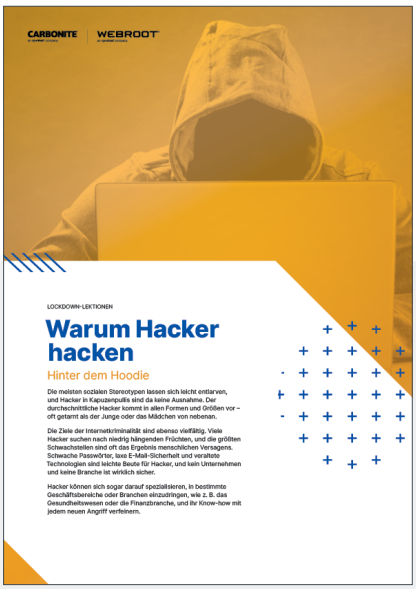
Der Stereotyp

Wie sieht ein Hacker aus? Stereotypen lehren uns, Hacker nur als ruchlose Individuen zu betrachten, die vor nichts zurückschrecken, um unaufhaltsamen Schaden anzurichten, aber das ist weit von der Realität entfernt. Entdecken Sie die Wahrheit hinter den Stereotypen und warum es Sie interessieren sollte.



Das Profil

Worauf sind Hacker aus? Hacker lassen sich typischerweise in drei verschiedene Kategorien einteilen: Black Hats, White Hats und Grey Hats (also schwarze, weiße und graue Hüte). Ihre Methoden und Motive variieren, von finanziellen Gewinnen bis hin zu Störungen, und manche hacken sogar nur zum Spaß. Erfahren Sie, warum es für Ihr Unternehmen wichtig ist.



Hinter dem Hoodie

Wer ist das Ziel von Hackern? Wenn Sie verstehen, warum Hacker es auf Ihr Unternehmen abgesehen haben und welche Methoden sie verwenden, um in Ihre Systeme einzudringen, können Sie Angriffe stoppen, bevor sie passieren.

CARBONITE
an opentext company

WEBROOT
an opentext company

LOCKDOWN-LEKTIONEN

Warum Hacker hacken

Der Stereotyp

Wenn Sie an einen Hacker denken, stellen Sie sich einen asozialen, jungen, Kapuzenpulli-tragenden Mann in einem dunklen Keller vor? Von Hollywood und den Mainstream-Medien popularisiert, ist dies das Bild, das viele von uns haben, obwohl es nicht ganz korrekt ist.

Diese Stereotypen lehren uns, Hacker nur als ruchlose Individuen zu betrachten, die vor nichts zurückschrecken, um unaufhaltsamen Schaden anzurichten. Die Realität ist jedoch, dass Hacken eine variable, vielfältige und höchst individuelle Praxis ist, und nicht alle Hacker sind Cyberkriminelle. Tatsächlich können einige Hacker sogar helfen, Ihre digitalen Abwehrmaßnahmen zu stärken!

Die Geschichte des Hollywood-Hackers

Das moderne Bild eines Hackers wurde durch populäre Filme und Fernsehsendungen geprägt, die den Mythos des jungen, rücksichtslosen Computergenies, das alles hacken kann, aufrechterhalten.

Die Ursprünge dieses Stereotyps beginnen eigentlich schon in den 1960er Jahren mit der britischen Komödie „The Italian Job“. Dank des Erfolgs des Films entwickelte sich das Stereotyp in den folgenden Jahrzehnten weiter, bis schließlich 2015 eine genauere Darstellung erschien.

„The Italian Job“ (1969)

Ein Räuber bekommt Hilfe von einer Gruppe der berüchtigtsten Computerhacker Großbritanniens, um Goldbarren zu stehlen. Dies war eine der ersten Hollywood-Darstellungen des Hackens als glamouröses und profitables Gewerbe.

„WarGames“ (1983)

Ein Highschool-Schüler hackt sich in einen Militärcomputer und aktiviert versehentlich das US-Atomwaffenarsenal. Einer der ersten Filme, der die verheerenden globalen Folgen eines einzigen Cyberangriffs vor Augen führt.

„Hacker“ (1995)

Eine jugendliche Hackergruppe muss beweisen, dass ein finsterer Superhacker ihnen eine Unterschlagung anhängt. Berühmt ist eine der ersten Darstellungen eines weiblichen Hackers, gespielt von Angelina Jolie.

„Matrix“ (1999)

Ein Computer-Hacker entdeckt, dass alles Leben auf der Erde vielleicht nur eine ausgeklügelte Fassade ist. Dieser Film trug dazu bei, das Klischee des schnell hackenden „Computergenies“ zu popularisieren, das wir heute kennen.

„Mr. Roboter“ (2015)

Ein junger Programmierer arbeitet tagsüber als Cybersicherheitsingenieur und nachts als anarchistischer Hacker. Gilt als eine der genauesten fiktionalen Darstellungen von realen Hackern.

eum qui bearcilit ipsam, ut facepero most velluptatius de coremporibus ipitiumqui occab ist, sit, sequisquo quas sed et aut accum non es eatum experum cullabo reperovid que sitis andel il incias magnaturibus doluptatem quas nobit unt evero exerchi llibus.

Fakt vs. Fiktion

Hollywood stellt Hacker oft entweder als rechtschaffene Selbstjustizler oder als böse Terroristen dar. Dies ist ein weit verbreiteter Irrglaube, der das Hacken romantisiert und dabei die realen Gefahren ignoriert; allerdings können genaue Darstellungen auch reale Probleme verursachen. Nachdem „WarGames“ 1983 Premiere hatte, unterzeichnete die US-Regierung den Computer Fraud and Abuse Act, um Hacker davon abzuhalten, Angriffe aus dem Film zu replizieren.

Während sich Filmemacher und Schauspieler Freiheiten bei ihren Darstellungen nehmen, bietet das Klischee des „Hollywood-Hackers“ einen kleinen Einblick in die wahren Motivationen von Hackern, wie Spionage, Diebstahl, Störung und sogar Altruismus.

Die Entlarvung der Hacker-Stereotypen

Hacker tragen viele „Hüte“ und haben unterschiedliche Mittel und Motive. Einer der größten Hacker-Mythen ist, dass die meisten Hacker Computergenies sind, während in Wirklichkeit viele Hacker Lowcode-Software verwenden, um Viren zu schreiben oder mit wenig bis gar keinen Programmierkenntnissen in Systeme einzubrechen.

Mythos: Alle Hacker sind „böse Schurken“, die darauf aus sind, Informationen zu stehlen.

Die Wahrheit: Computerhacker sind Personen, die Computer, Netzwerke oder andere Technologien und Fähigkeiten nutzen, um sich aus verschiedenen Gründen Zugang zu Computersystemen zu verschaffen.

Mythos: Alle Hacker sind männlich.

Die Wahrheit: Der durchschnittliche Hacker ist männlich und unter 35 Jahre alt[1], aber Hacker können jedes Alter, Geschlecht oder jede ethnische Zugehörigkeit haben.

Mythos: Alle Hacker sind Einzelgänger.

Die Wahrheit: Hacker sind koordiniert und arbeiten in einem breiten und komplexen Netzwerk. Sie haben oft Gehälter, feste Urlaubstage, Bonuszahlungen und Vertriebsvereinbarungen, die Wiederverkäuferportale und die Vermietung von Komponenten beinhalten. Es ist üblich, dass Hacker in größere Gruppen oder Organisationen eingebunden sind.

Mythos: Hacker müssen schnell arbeiten.

Die Wahrheit: Hacker kümmern sich normalerweise nicht um eine tickende Uhr, und viele gehen langsam und methodisch vor, um zu bekommen, was sie wollen.

Mythos: Es gibt sehr wenig Geld für das Hacken.

Die Wahrheit: Die durchschnittlichen Kosten einer Datenschutzverletzung liegen bei 3,92 Millionen US-Dollar[2] und 71 % der Datenschutzverletzungen sind finanziell motiviert. Der durchschnittliche Hacker kann bis zum 40-fachen des Durchschnittslohns eines Softwareingenieurs verdienen.[1]

Mythos: Hacker greifen nur große Unternehmen an.

Die Wahrheit: Kleine und mittelständische Unternehmen sind die Hauptziele. Mehr als 70 % der Cyberangriffe zielen auf kleine Unternehmen ab[3] und MSPs halten die Schlüssel in der Hand, wenn es um den Datenzugriff geht.

In Wirklichkeit sind nicht alle Hacker darauf aus, Ihr Unternehmen zu ruinieren. Die Motivationen der Hacker sind unterschiedlich und reichen von Störung bis hin zu finanziellem Gewinn oder einfach nur aus Spaß an der Sache.

„Cyberkriminelle nutzen Automatisierung, um die Arbeit eines ganzen Teams von Hackern zu erledigen! KI-basierte Cyberangriffe können mehrere Unternehmen auf einmal treffen und kein Unternehmen ist zu groß oder zu klein, um ein Ziel zu sein.“

Tyler Moffitt
Senior-Analyst für Bedrohungsforschung, Webroot

Wenn Sie die wahren Methoden und Motivationen hinter den Mythen besser verstehen, können Sie lernen, wie Sie Ihr Unternehmen absichern und Ihre Kunden vor den größten Bedrohungen von heute schützen können.

[1] HackerOne. „The 2019 Hacker Report.“ (August 2019)
[2] Sicherheitsinformationen. “2019 Cost of a Data Breach Report.” (Juli 2019)
[3] Verizon. “2019 Data Breach Investigations Report.” (Mai 2019)

CARBONITE
an opentext company

WEBROOT
an opentext company

LOCKDOWN-LEKTIONEN

Warum Hacker hacken

Das Profil

Hacker lassen sich typischerweise in drei verschiedene Kategorien einteilen: Black Hats, White Hats und Grey Hats (also schwarze, weiße und graue Hüte).

Black Hats sind Hacker, die die Computersicherheit in böswilliger Absicht verletzen, während White Hats bestehende Internet-Infrastrukturen testen, um Schlupflöcher oder Fehler im System zu finden, typischerweise um die Sicherheit zu verbessern. Grey Hats liegen irgendwo dazwischen und brechen oft illegal, aber ohne böswillige Absicht in Systeme ein.

Es gibt auch viele Untertypen von Black-, White- und Grey-Hat-Hackern mit unterschiedlichen Mitteln und Motiven, vom Skript-Kiddie für Anfänger bis zum Terroristen mit nationalem Hintergrund.

Black, White and Grey Hat Hacker

Warum kategorisieren wir Hacker nach ihren „Hats“? Die Analogie erinnert an die US-Western der 1930er und 40er Jahre, als die Guten weiße Cowboyhüte trugen und die Bösen schwarze. Obwohl dies eine zu starke Vereinfachung ist, hilft uns der Hat-Archetyp dabei, verschiedene Gruppen von Hackern anhand ihres Verhaltens und ihrer Motivationen zu definieren.

Black Hats

Black Hat Hacker, auch bekannt als Cyber-Kriminelle oder Bedrohungsakteure, verletzen die Computersicherheit in böswilliger Absicht oder zur persönlichen Bereicherung.

Talentierte Black Hats profitieren nicht nur davon, dass sie es auf Unternehmen und Privatpersonen abgesehen haben, sondern auch davon, dass sie ihre Tools an technisch weniger fähige Hacker („Skript-Kiddies“) verkaufen, z. B. Ransomware-as-a-Service oder Exploit-Kits zur Miete. Black Hats sind in der Regel hochqualifiziert, aber unterschätzen Sie Anfänger nicht. Mit den richtigen Werkzeugen können sie leicht ein großes Ziel treffen.

Warum hacken sie? Finanzieller Gewinn ist ein Hauptantrieb für Black Hat Hacker, und Hacken kann sehr profitabel sein. Black Hats verdienen ihr Geld in der Regel durch Diebstahl, Betrug, Erpressung und andere ruchlose Mittel.

White Hats

Auch als ethische Hacker bekannt, arbeiten White Hats daran, die bestehende Internet-Infrastruktur zu testen, um Schlupflöcher zu erforschen oder Bugs in einem System zu finden.

In der Vergangenheit waren White Hats entscheidend dafür, dass Unternehmen ein sicheres Netzwerk aufrechterhalten. Sie arbeiten oft als Angestellte oder Berater, in der Regel für Regierungen und große Unternehmen, obwohl einige mit MSPs und Sicherheitsfirmen zusammenarbeiten, um KMU zu helfen. Es gibt mindestens 300.000 registrierte White Hat Hacker auf der ganzen Welt.[1]

Warum hacken sie? Die Motivationen für White Hat sind unterschiedlich, obwohl Geld und Altruismus die Liste anführen. Der durchschnittliche zertifizierte ethische Hacker verdient etwa 91.000 Dollar pro Jahr.[2] „Bug Bounties“ sind eine Möglichkeit für White Hats, legal zu profitieren und Anerkennung zu erlangen.

Grey Hats

Grey Hacker sind diejenigen, deren Hacking-Praktiken zwar gegen ethische Standards verstoßen, aber im Allgemeinen ohne böswillige Absicht durchgeführt werden.

Ähnlich wie White Hats hacken sich Grey Hats oft in Computersysteme ein, um den Administrator oder Eigentümer darauf hinzuweisen, dass ihr Netzwerk eine oder mehrere Schwachstellen enthält, die behoben werden müssen. Im Gegensatz zu White Hats arbeiten Grey Hat Hacker jedoch nicht für ein offizielles Unternehmen und können Opfer erpressen, indem sie anbieten, Bugs gegen eine geringe Gebühr zu entfernen.

Warum hacken sie? Grey Hats mögen weniger bösartig sein als ihre Black Hat-Gegenstücke, aber Geld ist immer noch ein Hauptmotivator, obwohl einige zum Spaß hacken oder um ihre Programmierkenntnisse zu verbessern.

Hacker-Subtypen

Vom altruistisch motivierten „White Hat“ bis hin zum zutiefst finsteren „Black Hat“ gibt es eine große Bandbreite an Hacker-Persönlichkeiten, die jeweils von den Absichten geleitet werden, die hinter ihrem Hacking stehen.

Skript-Kiddies

Skript-Kiddies werden meist mit dem Stereotyp des „Hackers im Kapuzenpulli“ assoziiert und sind Programmieranfänger, die zwar über einige Programmierkenntnisse verfügen, denen es aber an Expertise fehlt. Sie verwenden in der Regel freie und quelloffene Software, die leicht im Dark Web zu finden ist, um Netzwerke zu infiltrieren, und können einen Black, White oder Grey Hat tragen.

Hacktivisten

Hacktivisten sind Grey Hat Hacker mit dem primären Ziel, durch Störung die öffentliche Aufmerksamkeit auf ein politisches oder soziales Anliegen zu lenken. Zwei der häufigsten Hacktivisten-Strategien sind der Diebstahl und die Veröffentlichung sensibler Informationen oder das Starten eines DDoS-Angriffs (Distributed Denial of Service). Eine der bekanntesten Hacktivistengruppen ist Anonymous, berüchtigt für das Herunterfahren der CIA-Website.

Red Hats

Red Hats sind die weißeren Schatten der Grey Hats, deren einziges Ziel es ist, die Bemühungen der Black Hat Hacker zu blockieren oder zu zerstören. Red Hats gelten als die „Selbstjustizler“ der Hackerwelt und versuchen, bösartige Angriffe mit ihren eigenen Werkzeugen zu unterbinden, anstatt den Verstoß zu melden.

Nationalstaat

Nationalstaatliche Hacker sind diejenigen, die Spionage, Social Engineering oder Computereinbrüche mit dem Ziel betreiben, geheime Informationen zu erlangen oder hohe Lösegelder zu fordern. Sie werden von Regierungen unterstützt und sind oft hoch entwickelt und gut ausgebildet.

Böswillige Insider

Ein Insider kann ein verärgerter aktueller oder ehemaliger Mitarbeiter sein, der Informationen stiehlt oder vernichtet, oder jemand, der von einem Konkurrenten angeheuert wurde, um Geschäftsgeheimnisse zu stehlen. Die wertvollsten Daten für einen böswilligen Insider sind Benutzernamen und Passwörter, die dann im Dark Web verkauft werden können, um einen saftigen Gewinn zu erzielen.

Das Verständnis der Hacker-Subtypen kann Ihnen helfen, potenzielle Bedrohungen sowie Möglichkeiten zu erkennen, wie Sie Hackerangriffe zum Schutz Ihres Unternehmens nutzen können.

„Während dies vor Jahren noch nicht der Fall war, hacken die meisten Black Hats heute aus monetären Gründen, weil es beim Hacken so viel Geld zu verdienen gibt. Auch White Hats, die ihre Kräfte für das Gute einsetzen, können einen Gewinn erzielen.“

Tyler Moffitt
Leitender Analyst für Bedrohungsforschung, Webroot

Hacker können jedes Unternehmen aus jedem Grund ins Visier nehmen! Das Verständnis ihrer Methoden und Motivationen kann Ihnen helfen, Ihr Unternehmen abzusichern und Ihre Kunden zu schützen.

[1] HackerOne. „The 2019 Hacker Report.“ (August 2019)
[2] PayScale. „Certified Ethical Hacker (CEH) Salary Data.“ (Dezember 2019)

CARBONITE an opentext company | WEBROOT an opentext company

LOCKDOWN-LEKTIONEN

Warum Hacker hacken

Hinter dem Hoodie

Die meisten sozialen Stereotypen lassen sich leicht entlarven, und Hacker in Kapuzenpullis sind da keine Ausnahme. Der durchschnittliche Hacker kommt in allen Formen und Größen vor – oft getarnt als der Junge oder das Mädchen von nebenan.

Die Ziele der Internetkriminalität sind ebenso vielfältig. Viele Hacker suchen nach niedrig hängenden Früchten, und die größten Schwachstellen sind oft das Ergebnis menschlichen Versagens. Schwache Passwörter, laxe E-Mail-Sicherheit und veraltete Technologien sind leichte Beute für Hacker, und kein Unternehmen und keine Branche ist wirklich sicher.

Hacker können sich sogar darauf spezialisieren, in bestimmte Geschäftsbereiche oder Branchen einzudringen, wie z. B. das Gesundheitswesen oder die Finanzbranche, und ihr Know-how mit jedem neuen Angriff verfeinern.

Wen sie verletzen: Die Tricks der Branche

Ähnlich wie beim heutigen Kapuzenpulli-Stereotyp herrscht auch bei kleinen und mittelständischen Unternehmen der gefährliche Irrglaube vor, dass Hacker es nur auf große Unternehmen abgesehen haben. Tatsächlich ist aber jedes Unternehmen, das mit personenbezogenen Daten, Bankkonten, Gesundheitsdaten und anderen sensiblen Informationen umgeht, gefährdet. Die einfache Wahrheit ist, dass der Großteil des kriminellen Geldes mit kleinen und mittleren Unternehmen in zentralen Branchen verdient wird. Wer ist also ein Ziel?

Managed Service Provider

MSPs verfügen über eine Menge wertvoller Daten für eine Vielzahl von Kunden aus verschiedenen Branchen, was sie zu erstklassigen Zielen macht. Insel-Hopping ist eine gängige Hacking-Technik, bei der Hacker über gestohlene Anmeldedaten von einem Unternehmen zum anderen springen. MSPs und ihre KMU-Kunden sind beide potenzielle Ziele dieser Angriffe.

Organisationen im Gesundheitswesen

Krankenhäuser, Physiotherapiepraxen, Kinderärzte, Chiropraktiker und andere Gesundheitspraxen sind aufgrund ihrer chaotischen und manchmal laxen Sicherheitspraktiken leichte Ziele für Cyberkriminalität. Medizinische Daten und Forschung sind für den richtigen Käufer sehr wertvoll. Im Dark Web können allein Patientenakten für bis zu 1.000 Dollar oder mehr verkauft werden.[1]

Kommunen, Infrastruktur und Versorgungsunternehmen

Auch Städte können Opfer von Cyberangriffen werden. Nicht nur die massiven Datenmengen, die in städtischen Systemen gespeichert sind, sind attraktiv, sondern Hacker können auch störende Ransomware-Angriffe starten, bei denen Infrastrukturen oder Versorgungseinrichtungen abgeschaltet werden, bis die geforderte Summe gezahlt wird. Viele Städte setzen immer noch auf veraltete Bestandssysteme, die anfällig für Malware oder Ransomware sind.

Staatliche Stellen

Lokale und nationale Regierungen sind aus einer Vielzahl von Gründen primäre Ziele für Cyberkriminelle, insbesondere für nationalstaatliche Terroristen. Kleine Regierungen und lokale Behörden generieren Unmengen an sensiblen Informationen, während große Regierungen Opfer einer landesweiten Störung werden können.

Finanzeinrichtungen

Banken, Kreditgenossenschaften und andere Finanzinstitute sind seit Langem ein Ziel für Hacker, da sie eine Fülle von Daten und Geld besitzen. Tatsächlich waren 2018 über 25 % aller Malware-Angriffe auf Banken gerichtet – mehr als auf jede andere Branche.[2] Darüber hinaus hat die Automatisierung es Cyberkriminellen ermöglicht, fortschrittliche Angriffe auf Finanzinstitute in großem Umfang durchzuführen.

Prominente, Politiker und hochkarätige Marken

Hacktivisten, die politisch, wirtschaftlich oder sozial motiviert sind, suchen sich Prominente, Politiker und andere prominente Organisationen als Ziele aus. Sie können sogar versuchen, Personen des öffentlichen Lebens oder Unternehmen in Verlegenheit zu bringen, indem sie sensible, geschützte oder geheime Daten stehlen und verbreiten, um die Öffentlichkeit zu stören, oder um sich durch Erpressung privat finanziell zu bereichern.

So schützen Sie sich vor böswilligen Hackern

Die einzige Voraussetzung, um ein Ziel zu werden, ist, etwas zu haben, was Hacker wollen, was alle Unternehmen in Gefahr bringt. Glücklicherweise können das Bewusstsein für Bedrohungen und ein proaktiver Ansatz für die Sicherheit einen großen Beitrag zur Sicherheit Ihres Unternehmens leisten.

Denken Sie wie ein Hacker

Sicherheitsbewusstsein ist ein wichtiger Bestandteil effektiver Cybersicherheit. Tatsächlich hat Webroot in einer eigenen Studie herausgefunden, dass Sicherheitsschulungen die Klicks auf Phishing-Links um 70 % reduzieren, wenn sie regelmäßig durchgeführt werden. Das Verständnis von Hackerpraktiken und -motivationen kann Ihnen helfen, potenzielle Bedrohungen vorherzusehen und Angriffe zu vereiteln.

Sichern Sie zuerst Ihr Geschäft

Die richtigen Sicherheitsschichten können Sie vor Bedrohungen von allen Seiten schützen. Sehen Sie sich die kostenlosen Schulungsvideos, Podcasts und Cybersecurity-Leitfäden von Webroot in unserem **Lockdown Lessons Resource Center** an, um zu erfahren, wie Ihr Unternehmen von mehrschichtiger Cybersecurity profitieren kann.

Nutzen Sie die automatische Erkennung von Bedrohungen

Da moderne Angriffe immer komplexer werden und in großem Umfang automatisiert werden, wird Ihr Unternehmen immer stärker ins Visier geraten. Der beste Weg, gezielte Angriffe zu bekämpfen, besteht darin, Bedrohungen, die durchkommen, schnell und automatisch zu beseitigen. Automated Detection and Response (ADR)-Lösungen verbessern die Erkennungsgenauigkeit und Reaktionsgeschwindigkeit, die für die Abwehr von Angriffen entscheidend sind.

Schützen Sie Ihre Kunden

Ihre Kunden sind möglicherweise nicht ausreichend für den Umgang mit einer Sicherheitsverletzung gerüstet. MSPs sind in einer einzigartigen Position, um KMU-Kunden qualitativ hochwertige, umfassende Schulungen zum Sicherheitsbewusstsein zusammen mit Cybersecurity-Expertise und automatisiertem Schutz anzubieten. KMU, die ihre Sicherheitslage verbessern wollen, sollten auch Partnerschaften mit MSPs und anderen Managed Security Providern eingehen, um ihre eigenen Netzwerke und Systeme zu sichern.

Während Hacker unterschiedliche Mittel und Motive haben, ist Ihr Unternehmen für Black Hats und andere böswillige Eindringlinge der Schlüssel zum Königreich. Es liegt an Ihnen, deren Methoden zu kennen und Ihr Unternehmen und Ihre Kunden vor fortschrittlichen Bedrohungen zu schützen.

„Einer der größten Trends, den wir in den letzten Jahren gesehen haben, ist die Spezialisierung der kriminellen Hacker."

Kelvin Murray
Leitender Bedrohungsforscher, Webroot

Wenn Sie verstehen, warum Hacker hinter Ihrem Unternehmen her sind und welche Methoden sie verwenden, um in Ihre Systeme einzudringen, können Sie Angriffe stoppen, bevor sie passieren.

[1] CBS News. „Hackers are stealing millions of medical records – and selling them on the dark web." (Februar 2019)
[2] Forrester. „The Total Economic Impact of the IntSights External Threat Protection Suite." (Oktober 2019)
[3] Webroot. „Webroot 2019 Threat Report." (Februar 2019)

Fazit

Obwohl Hacker vielfältig sind und das Hacken als Beruf komplexer ist, als vielen bewusst ist, bleiben die Ziele von Cyberangriffen gleich. Die Realität ist, dass jedes Unternehmen ein potenzielles Ziel für böswillige Hacker ist – auch Sie und Ihre Kunden! Cyberattacken gegen MSPs und KMU nehmen zu. Daher ist es unerlässlich, sich gegen alle Arten von Bedrohungen zu schützen. Die Absicherung Ihres Unternehmens beginnt damit, dass Sie sich über Hacker und ihre Methoden informieren, aber damit ist es nicht getan. Schützen Sie Ihre Kunden mit den fortschrittlichsten Cybersicherheitslösungen, die helfen, Sicherheitslücken zu schließen und Bedrohungen schnell zu beseitigen.

Warten Sie nicht, um Ihr Unternehmen zu schützen!

Was Sie nicht wissen, kann Ihnen Schaden zufügen. Cyberattacken gegen MSPs und KMU sind auf dem Vormarsch. Starten Sie eine kostenlose Webroot-Testversion und sehen Sie selbst, wie unsere Lösungen Ihnen helfen können, Bedrohungen zu verhindern und Ihr Wachstum zu maximieren.

Kontaktieren Sie uns, um mehr zu erfahren

E-Mail: DACH-smbc@opentext.com

Telefon: +49 (0)2162 91980 20

Über Carbonite und Webroot

Carbonite und Webroot, Unternehmen von OpenText, nutzen die Cloud und künstliche Intelligenz, um umfassende Cyber-Resilience-Lösungen für Unternehmen, Privatpersonen und Managed Service Provider anzubieten. Cyberresilienz bedeutet, dass Systeme trotz Cyberangriffen und Datenverlusten jederzeit aktiv und betriebsbereit sind. Deshalb haben wir unsere Kräfte gebündelt, um Lösungen für den Schutz von Endpunkten, den Schutz von Netzwerken, Schulungen zum Sicherheitsbewusstsein und Lösungen für Datensicherung und Disaster Recovery sowie Threat Intelligence Services anzubieten, die von marktführenden Technologieanbietern weltweit genutzt werden. Webroot nutzt die Leistungsstärke des maschinellen Lernens zum Schutz von Millionen von Unternehmen und Einzelpersonen und sichert die vernetzte Welt. Carbonite und Webroot sind weltweit in Nordamerika, Europa, Australien und Asien tätig. Erfahren Sie unter carbonite.com und webroot.com mehr über Cyberresilienz.