SOPHOS
Security made simple.

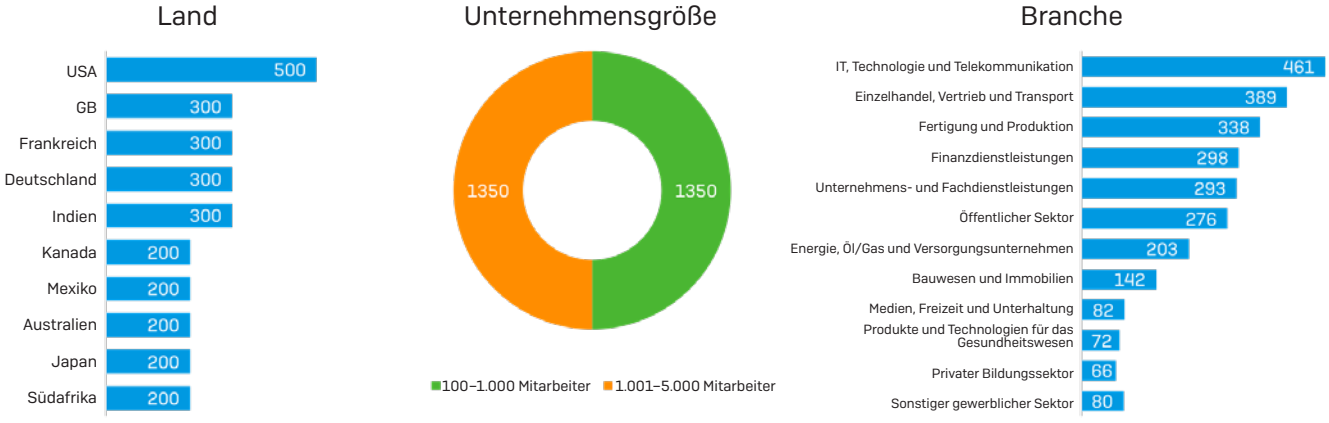
Status quo der Endpoint Security

Eine unabhängige Studie unter 2.700 mittelständischen Unternehmen auf allen fünf Kontinenten

Einführung

Ende des Jahres 2017 gab Sophos eine unabhängige, globale Forschungsstudie in Auftrag, um Einblicke in den Status quo der Endpoint Security in mittelständischen Unternehmen weltweit zu gewinnen. Im Rahmen des umfassenden Projekts wurden die wichtigsten Entwicklungen und Probleme beleuchtet: Sicherheitsverstöße, Technologienutzung, Einstellung zu Bedrohungen sowie geplante Investitionen.

An der vom führenden britischen Forschungsinstitut Vanson Bourne durchgeführten Studie beteiligten sich 2.700 IT-Manager in Unternehmen mit 100 bis 5.000 Usern in 10 Ländern auf 5 Kontinenten.



Demographie der Umfrage: Anzahl der Befragten nach Land, Unternehmensgröße und Branche

Das daraus resultierende White Paper liefert wertvolle Einblicke in die aktuellen Probleme im Bereich Cybersecurity in Unternehmen: Von Ransomware zu Exploits und Machine Learning zeigt der Guide die Erfahrungen und Zukunftspläne von IT-Managern weltweit auf. Zudem gibt das Paper Aufschlüsse darüber, wie Unternehmen diese Herausforderungen meistern.

Der Schatten der Ransomware

Kurzfassung

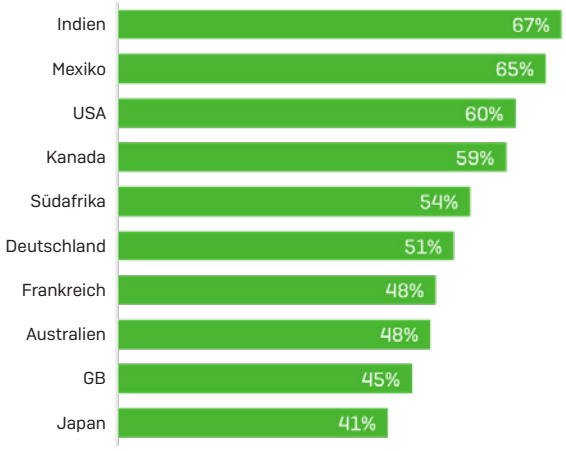
- 54 % der Unternehmen wurden im letzten Jahr Opfer von Ransomware
- Im Durchschnitt zwei Ransomware-Angriffe pro Unternehmen
- Durchschnittliche Folgekosten je betroffenem Unternehmen in Höhe von ca. $ 133.000 USD
- Am häufigsten von Angriffen betroffen war das Gesundheitswesen, gefolgt von Fachdienstleistungen und Einzelhandel
- Die höchste Infektionsrate verzeichnete Indien, darauf folgen Mexiko, die USA und Kanada
- 77 % der Unternehmen nutzten zum Zeitpunkt des Angriffs aktualisierte Endpoint-Security
- 54 % der Unternehmen haben keine spezielle Anti-Ransomware-Software im Einsatz

Wiederholte Angriffe

Nach wie vor stellt Ransomware ein enormes Problem weltweit dar. 54 % der befragten Unternehmen waren im letzten Jahr davon betroffen. 31 % unserer Umfrageteilnehmer rechnen in Zukunft mit Ransomware-Angriffen. Im Durchschnitt fielen Unternehmen in den letzten 12 Monaten sogar zwei Mal Ransomware-Angriffen zum Opfer.

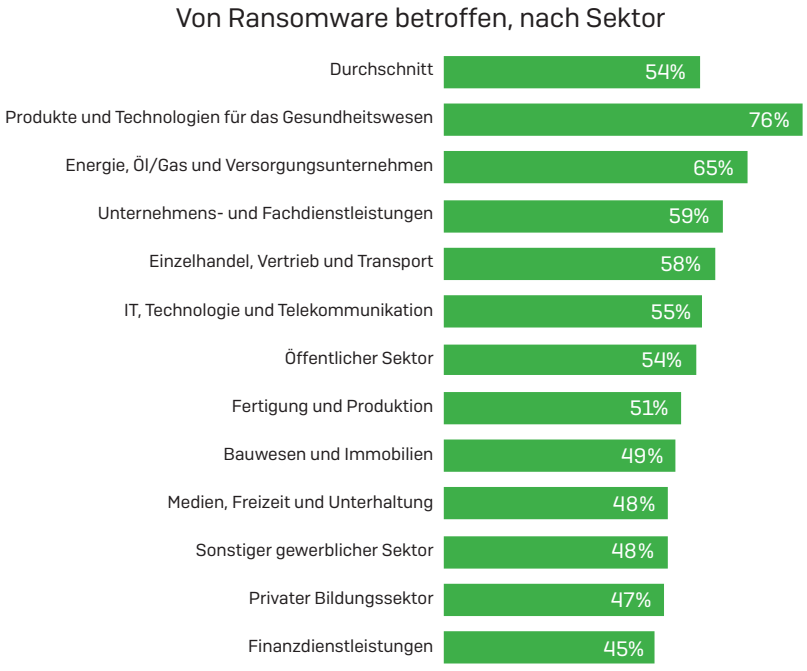
Ransomware legte Unternehmen in allen Ländern lahm. Das Ausmaß der Vorfälle variierte jedoch sehr nach Region. An der Spitze der Ransomware-Opfer stand Indien: Ganze zwei Drittel (67 %) der Befragten waren im vergangenen Jahr von Ransomware betroffen. Am unteren Ende der Skala lag Japan: Hier waren 41 % der Unternehmen Opfer von Ransomware. Ein wichtiger Faktor ist hierbei wahrscheinlich die Sprache – Ransomware-Angriffe gehen häufig von Phishing-E-Mails aus. Eine englischsprachige E-Mail kann in mindestens sechs der befragten Länder genutzt werden. Eine E-Mail auf Japanisch beschränkt sich hingegen auf eine Region. Die Schwierigkeit seiner Sprache bietet Japan in diesem Fall Schutz vor Angriffen.

Von Ransomware betroffen, nach Land



% der Unternehmen, die in den letzten zwölf Monaten von Ransomware betroffen waren

Die Anfälligkeit für Ransomware-Angriffe ist sehr stark branchenabhängig. Der Gesundheitssektor sticht klar hervor; 76 % der Befragten wurden im vergangenen Jahr Opfer von Angriffen. Am anderen Ende der Skala liegen die Finanzdienstleistungen mit dem geringsten Vorfallsrisiko. Und dennoch steht auch diese Branche unter enormem Druck: 45 % der Befragten waren berichteten von Ransomware-Angriffen.



% der Unternehmen, die in den letzten zwölf Monaten von Ransomware betroffen waren, nach Sektor

Sowohl im Gesundheitswesen als auch in der Finanzdienstleistungsbranche werden sehr sensible Daten verarbeitet. Das Gesundheitswesen gilt jedoch als leichtes Ziel, was die erhöhte Angriffshäufigkeit erklärt. Und in der Tat sind die IT-Infrastrukturen im Gesundheitswesen nicht selten veraltet und die Ressourcen für die IT-Security sind knapp: Sicherheitslücken sind die logische Konsequenz. Zudem gehen Cyberkriminelle davon aus, dass Organisationen im Gesundheitswesen Lösegeldforderungen mit höherer Wahrscheinlichkeit nachgehen.

Interessanterweise ist die Unternehmensgröße für Hacker nicht ausschlaggebend. Die Angriffswahrscheinlichkeit bewegten sich bei kleineren und größeren Unternehmen, die an der Umfrage teilnahmen, in etwa auf demselben Niveau: 50 % der Unternehmen mit 100 bis 1.000 Benutzern waren bereits von Ransomware betroffen. Bei Unternehmen zwischen 1.001 und 5.000 Benutzern lag der Prozentsatz bei 58 %. Egal ob groß oder klein – alle Unternehmen sind potenzielle Opfer.

Herkömmlicher Endpoint-Schutz allein ist nicht genug

Mehr als drei Viertel (77 %) der Ransomware-Opfer nutzen bereits aktuelle Endpoint-Security. Leider müssen Unternehmen nicht selten schmerzliches Lehrgeld bezahlen und feststellen, dass Ransomware dedizierten Schutz erfordert.

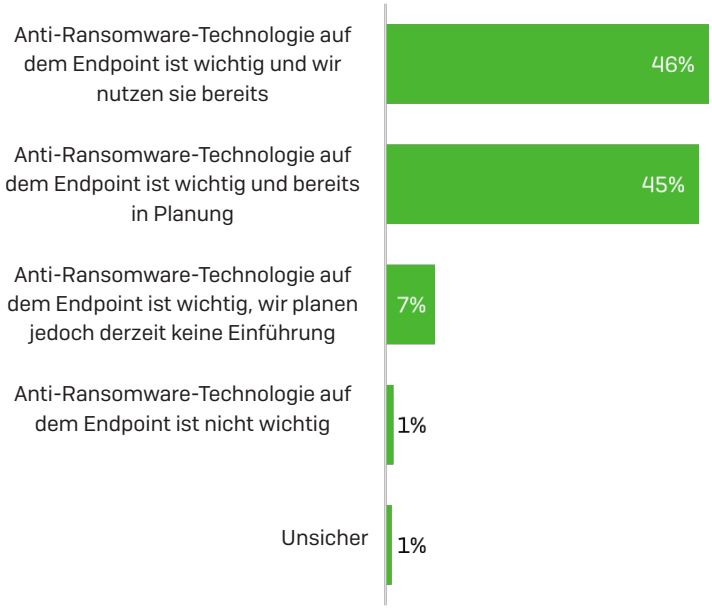
Prozent der Unternehmen, die in den letzten 12 Monaten von Ransomware betroffen waren und zum Zeitpunkt des Angriffs aktualisierte Endpoint-Security nutzten

Endpoint-Schutzniveau	Gesamt
Nutzen aktualisierten Endpoint-Schutz	77 %
Nutzen keinen aktualisierten Endpoint-Schutz	21 %
Unsicher	1 %

Basis: 1468

Angesichts der namhaften Ransomware-Angriffe „WannaCry“ und „Petya“ des Jahres 2017 und der Vielzahl der Betroffenen überrascht es kaum, dass sich fast alle Befragten (98 %) einig waren, dass Anti-Ransomware-Technologie auf dem Endpoint wichtig ist. 50 % der Unternehmen nutzen solche Technologien jedoch nicht und sind somit einem größeren Angriffsrisiko ausgesetzt.

Ansicht der Befragten zur Aufnahme dedizierter Anti-Ransomware-Technologie in den Endpoint-Schutz des Unternehmens



Das Investitionsniveau in Ransomware variiert erheblich von Sektor zu Sektor. Der Sektor „Energie, Öl/Gas und Versorgungsunternehmen“ und das Gesundheitswesen investierten am meisten in Technologie zum Schutz vor Ransomware. Beide gelten bei Cyberkriminellen als lukrative Ziele. Auch setzen sie spezielle, kostspielige Ausrüstung ein, wie etwa die MRT-Scanner im Gesundheitswesen oder die Bohrer in der Ölindustrie.

Bei den Medien, dem öffentlichen Sektor sowie dem privaten Bildungswesen ist die Investitionswahrscheinlichkeit in Anti-Ransomware-Technologie am geringsten. Das hat verschiedene Ursachen. Häufig werden jedoch – insbesondere im öffentlichen Sektor – Budgetzwänge oder ein Mangel an Informationen angeführt. Beschränkte IT-Ressourcen erklären zudem, warum Unternehmen in diesen Branchen noch keine Anti-Ransomware-Lösungen nutzen.

Ansicht der Befragten zur Aufnahme dedizierter Anti-Ransomware-Technologie in den Endpoint-Schutz des Unternehmens, nach Sektor

	Durchschnitt	Unternehmens- und Fachdienstleistungen	Bauwesen und Immobilien	Energie, Öl/Gas und Versorgungsunternehmen	Finanzdienstleistungen	Sicherheitsstatus	IT, Technologie, Telekommunikation	Fertigung	Medien, Freizeit, Unterhaltung	Öffentlicher Sektor	Privater Bildungssektor	Einzelhandel, Vertrieb und Transport	Sonstiges
Anti-Ransomware-Technologie auf dem Endpoint ist wichtig und wir nutzen sie bereits	**46 %**	47 %	46 %	53 %	52 %	53 %	44 %	46 %	38 %	39 %	35 %	46 %	51 %
Anti-Ransomware-Technologie auf dem Endpoint ist wichtig und bereits in Planung	**45 %**	42 %	46 %	42 %	41 %	42 %	47 %	46 %	51 %	50 %	45 %	43 %	36 %

Der Sonderfall Gesundheitswesen: Hauptziel von Angriffen, größtes Investitionsvolumen in Prävention

Die Lage im Gesundheitswesen ist interessant. Der Sektor stellt das wahrscheinlichste Angriffsziel (76 %) dar und dennoch wird hier am meisten in Schutz vor Ransomware investiert (53 %, gleichauf mit Energie, Öl/Gas und Versorgungsunternehmen).

Wie erklärt sich dieser Widerspruch? Zum einen liegt es daran, dass Cyberkriminelle das Gesundheitswesen weiterhin als ein leichtes Ziel ansehen und daher ein unverhältnismäßig hoher Anteil der Angriffe auf den Sektor entfällt. Zudem läuft die ältere Technologie, die hier zum Einsatz kommt (wie etwa die bereits erwähnten MRT-Geräte) häufig unter alten Betriebssystemen.

Einen weiteren Faktor stellen beschränkte Ressourcen in diesem Bereich dar. Mangel an Personal, Hardware und Software führen zu lückenhafter IT-Sicherheit. Es kann also durchaus vorkommen, dass nur Teile einer Organisation über Ransomware-Schutz verfügen. Und so hat Malware immer eine Chance.

Hinzu kommen ferner Qualitätsprobleme. Nicht alle Anti-Ransomware-Lösungen sind gleich und bieten nicht die gleiche Effektivität in der Abwehr von Angriffen.

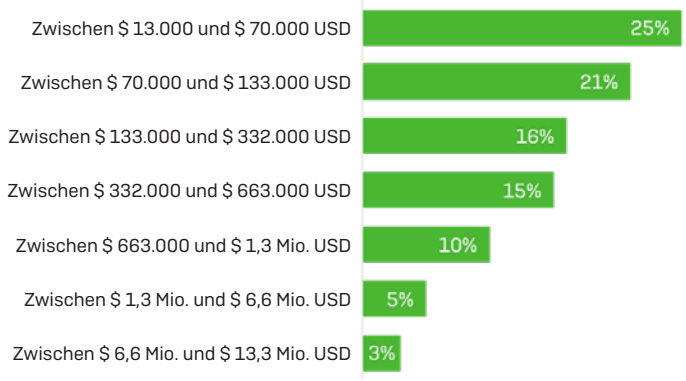
Glücklicherweise hat das Gesundheitswesen aus den negativen Erfahrungen gelernt und investiert nun in Anti-Ransomware-Technologie.

Die hohen Folgekosten eines Ransomware-Angriffs

In Zusammenhang mit Ransomware entstehende Kosten gehen weit über eventuell gefordertes Lösegeld hinaus. Unsere Umfrage hat ergeben, dass die finanziellen Auswirkungen eines Ransomware-Angriffs – einschließlich Ausfallzeiten, investierte Arbeitsstunden, entgangene Geschäftschancen und Lösegeld – viele Tausende Dollar, Euro, Yen, Pfund, Pesos, Rand oder Rupien beträgt.

Im Durchschnitt liegen die durch Ransomware-Angriffe entstehenden Kosten bei beinahe $ 133.000 USD. Dabei meldeten 51 % der Unternehmen höhere und 49 % niedrigere Kosten. In den meisten Fällen lagen die Kosten zwischen $ 13.000 und $ 70.000 USD. Fast der Hälfte der Befragten (46 %) entstanden Kosten in Höhe von $ 13.000 und $ 133.000 USD.

Ungefährer finanzieller Aufwand, der den befragten Unternehmen durch Ransomware-Angriffe entstanden ist (unter Berücksichtigung von Ausfallzeiten, Arbeitsstunden, Geräte- und Netzwerkkosten, entgangenen Geschäftschancen, Lösegeld usw.)



Die Umfrage hat zudem **ergeben, dass die Kosten, die US-Unternehmen aus Ransomware entstehen, das BIP von Jamaika übersteigen.** Auf der Basis der Umfrageergebnisse belief sich der US-Unternehmen mit 100 oder mehr Mitarbeitern aus Ransomware entstandene finanzielle Aufwand auf 18,6 Milliarden $ USD. Nur zum Vergleich: Das BIP von Jamaika lag in 2016 bei $ 14 Milliarden USD.

Unsere Perspektive

Obgleich eine Reihe von Ransomware-Angriffen im Jahr 2017 die Schlagzeilen beherrschte, verfügen im Jahr 2018 viele Unternehmen bestenfalls über unzureichenden Schutz vor Ransomware. Unternehmen, die bereits Anti-Ransomware-Technologie in Erwägung ziehen, müssen ferner darauf achten, dass die gewählte Lösung spezifische Anti-Ransomware-Funktionen aufweist und nicht nur allgemeinen Schutz vor Bedrohungen bietet.

Wir sind der Meinung, dass es an der Zeit ist, die Effektivität von Anti-Ransomware-Produkten sowie ihre Fähigkeit, bislang unbekannte Bedrohungen abzuwehren in unabhängigen Tests prüfen zu lassen, damit IT-Experten fundierte Entscheidungen treffen können.

Wir gehen im Jahr 2018 aufgrund von Ransomware-as-a-Service (RaaS) und dem Comeback von Würmern sogar von noch mehr Ransomware-Angriffen aus. Vor diesem Hintergrund empfiehlt sich, Technologie-Upgrades nicht herauszuzögen. Sichern Sie sich rechtzeitig dedizierten Schutz vor Ransomware.

Unsere Empfehlungen

Jedes Unternehmen steht im Zielvisier von Ransomware. Vorbereitung ist alles. Unternehmen aller Größen waren von Ransomware-Angriffen betroffen.

Der erste Schritt liegt in der Aufklärung. Informieren Sie sich und Ihre Endbenutzer. Schulen Sie Ihre Mitarbeiter durch Simulationen, damit diese Angriffe erkennen können. Nicht selten sind Endbenutzer – und menschliches Fehlverhalten – das schwächste Glied Ihrer IT-Sicherheit. Gut geschulte Mitarbeiter sind hingegen Ihr größtes Kapital.

Informieren Sie sich über die Optionen der angebotenen Technologien. Herkömmlicher Virenschutz sowie Endpoint Security wehren lediglich bekannte Ransomware ab. Angesichts der rasanten Geschwindigkeit, in der neue Malware entwickelt und in Umlauf gebracht wird, benötigen Sie dedizierten Schutz vor Ransomware, um Zero-Day-Angriffen Einhalt zu gebieten.

Rüsten Sie Ihre Technologie auf. Lösungen zur Abwehr von Ransomware und Prävention von Exploits sind in den letzten Jahren beträchtlich weiterentwickelt worden. Und vergessen Sie nicht: Die Investition in entsprechende Technologie liegt weit unter dem mit Angriffen einhergehenden finanziellen Aufwand. Sie sparen Geld und Ihre Reputation bleibt intakt, wenn Sie sich vor Angriffen schützen.

Abwehr von Exploits

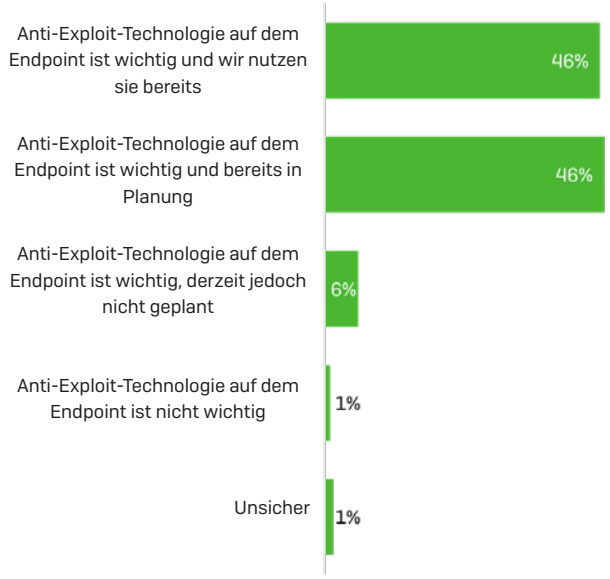
Kurzfassung

- 54 % der Unternehmen nutzen keine Anti-Exploit-Technologie
- Zwei Drittel der IT-Manager wissen nicht, was Anti-Exploit-Technologie ist
- Das Verständnis von Anti-Exploit-Technologien ist in den USA am größten, gefolgt von Mexiko

Stoppen Sie den Exploit, so stoppen Sie auch den Angriff

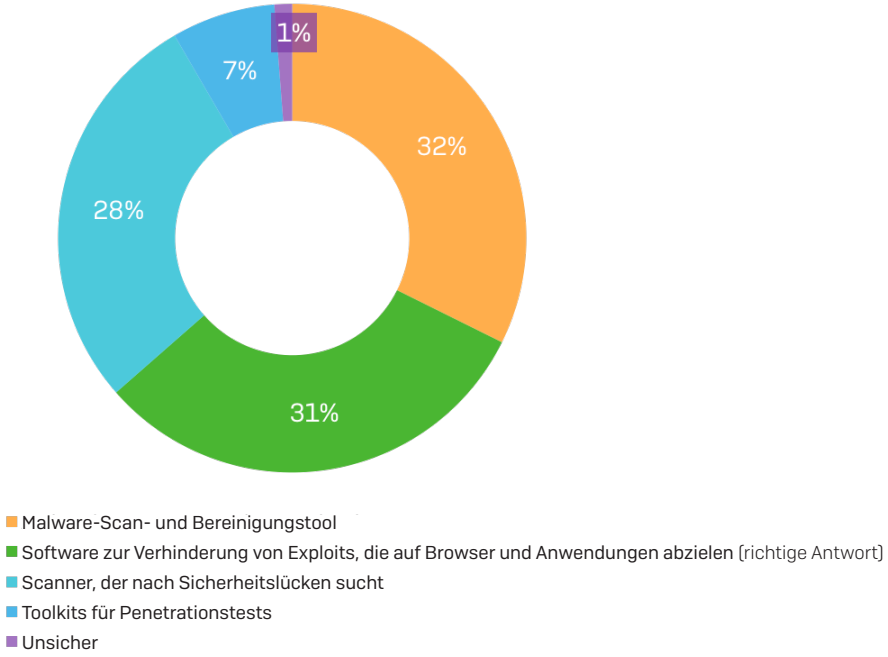
Exploits, über die sich Hacker Sicherheitslücken in seriöser Software zunutze machen, kamen in vielen hochkarätigen Angriffen zum Tragen. Weltweit machte der im WannaCry-Ransomware-Angriff genutzte Exploit „Eternal Blue“ Schlagzeilen. Vor diesem Hintergrund überrascht es auch nicht, dass fast alle Befragten (98 %) sich einig waren, dass Anti-Exploit-Technologie auf dem Endpoint wichtig ist. Mehr als die Hälfte der Umfrageteilnehmer (54 %) gab hingegen an, dass sie keine Anti-Exploit-Technologie auf dem Endpoint einsetzen und so anfällig für Angriffe sind.

Ansicht der Befragten zur Aufnahme dedizierter Anti-Exploit-Technologie in den Endpoint-Schutz des Unternehmens



Zwar gaben 46 % an, bereits Anti-Exploit-Technologie zu nutzen, weniger als ein Drittel (31 %) der Befragten konnte Anti-Exploit-Software jedoch genau definieren. Dieser Umstand deutet darauf hin, dass ein erheblicher Anteil der Unternehmen fälschlicherweise davon ausgehen, dass sie vor dem gängigen Angriffsverfahren geschützt sind. In Wirklichkeit sind sie jedoch enormen Risiken ausgesetzt.

Welche Beschreibung trifft am ehesten auf Anti-Exploit-Software zu?



Das Verständnis variierte je nach Region: Die USA führten die Liste mit 39 % korrekten Definitionen an. In Frankreich lag der Wert bei lediglich 22 %. Überraschenderweise war der Kenntnisstand zum Thema Anti-Exploit-Technologie in kleinen Unternehmen größer: 34 % der Unternehmen mit 100 bis 1.000 Benutzern konnten den Begriff richtig definieren. In der Gruppe mit 1.001 bis 5.000 Benutzer gelang dies nur 29 %.

Anti-Exploit-Software richtig definiert

GB	Frankreich	Deutsch-land	USA	Kanada	Mexiko	Indien	Australien	Japan	Südafrika
35 %	22 %	32 %	39 %	26 %	35 %	28 %	34 %	26 %	30 %

% der Befragten, die die Definition von Anti-Exploit-Software zuordnen konnten, nach Land

Unsere Empfehlungen

Angesichts der Tatsache, dass Exploits in modernen Angriffen vermehrt zum Einsatz kommen und das Angebot an Anti-Exploit-Technologie beschränkt ist, besteht dringend Handlungsbedarf. Wer die Exploit-Thematik nicht versteht, sollte sich damit befassen. Und selbst wenn Sie mit der Thematik vertraut sind, empfiehlt sich, Ihre Kenntnisse aufzufrischen und sich mit den neuesten Methoden zu beschäftigen.

Jetzt ist der perfekte Zeitpunkt für ein Technologie-Upgrade. Stellen Sie sicher, dass Sie Ihre Security-Lösungen vor den in Malware-Angriffen verwendeten Exploit-Techniken schützt.

Komplexe Bedrohungen und Machine Learning

Kurzfassung

- 87 % stimmen zu: Bedrohungen sind im Verlauf des letzten Jahres komplexer geworden
- 60 % gaben an, dass ihre aktuelle Cyberabwehr unzulänglich ist
- 60 % planen die Einführung prädiktiver Technologien wie Machine Learning oder Deep Learning im nächsten Jahr
- In Kanada, Indien und Mexiko ist die Akzeptanz von Machine Learning am größten
- Indien sieht das Potenzial von Machine Learning am optimistischsten

Sie sind nicht allein

Die Umfrage bestätigte, dass der Umgang mit den komplexen Malware-Angriffen von heute IT-Manager weltweit vor eine immer größere Herausforderung stellt:

- 83 % stimmen zu, dass die Abwehr von Malware-Bedrohungen im Verlauf des letzten Jahres schwieriger wurde
- 87 % stimmen zu, dass Malware-Bedrohungen im Verlauf des letzten Jahres zunehmend komplexer wurden

Zwar wird diese Ansicht in allen befragten Regionen vertreten, in Japan ist der Wandel jedoch am meisten spürbar: 92 % geben an, dass sich die Abwehr von Bedrohungen schwieriger gestaltet und 97 % stimmen zu, dass diese an Komplexität zugenommen haben.

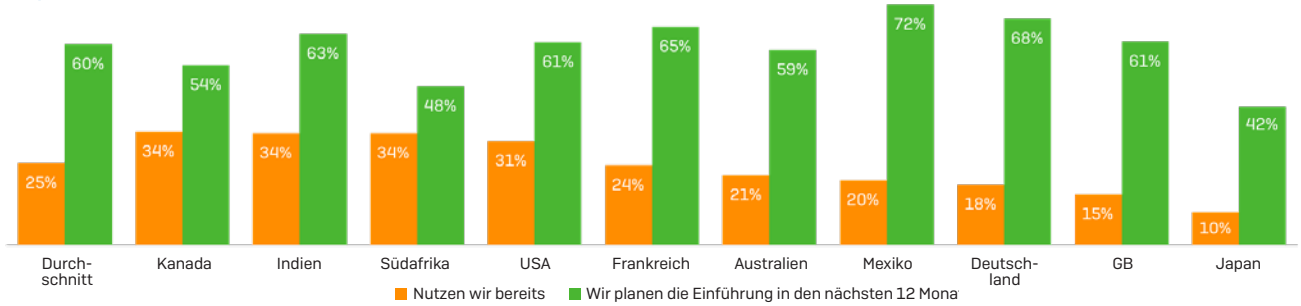
	Stimmen zu, dass die Abwehr von Bedrohungen im Verlauf des letzten Jahres schwieriger wurde	Stimmen zu, dass Malware-Bedrohungen im Verlauf des letzten Jahres zunehmend komplexer wurden
GB	85 %	89 %
Frankreich	74 %	79 %
Deutschland	77 %	87 %
USA	88 %	90 %
Kanada	76 %	82 %
Mexiko	81 %	86 %
Indien	89 %	88 %
Australien	85 %	84 %
Japan	92 %	97 %
Südafrika	85 %	89 %

Herkömmliche Endpoint-Technologien sind den ausgeklügelten Bedrohungen von heute häufig nicht gewachsen. Ganze 60 % der Befragten gaben an, dass ihre aktuelle Endpoint-Security den Angriffen des letzten Jahres nicht standhalten kann. Die Befragten in allen Regionen und Unternehmensgrößen waren sich durchaus einig. Im Gesundheitswesen wurde das geringste Vertrauen in die Endpoint-Lösung verzeichnet: 72 % erachten ihre Security als unzulänglich. Angesichts der Anfälligkeit des Sektors für Ransomware überrascht dies wenig.

Kein Wunder also, dass Unternehmen zunehmend Interesse an präventiven Technologien zur Bedrohungsabwehr, wie Deep Learning und Machine Learning, zeigen, um sich vor bislang unbekannten Bedrohungen zu schützen. 85 % der Unternehmen nutzen bereits (25 %) prädiktive Technologien oder planen im nächsten Jahr ihre Einführung (60 %).

Die Pläne zur Umsetzung prädiktiver Technologien variieren laut unserer Umfrage stark je nach Region. An der Spitze stehen Kanada, Indien und Mexiko. In diesen Ländern nutzen bereits 34 % der Befragten prädiktive Technologien wie Deep Learning und Machine Learning. Mexiko hat die umfangreichsten Pläne: zur 72 % planen eine Einführung der Technologien im Verlauf des nächsten Jahres. In Japan fällt die Akzeptanz prädiktiver Technologien unter den befragten Ländern am niedrigsten aus: Lediglich 10 % nutzen sie bereits und 41 % planen eine Einführung.

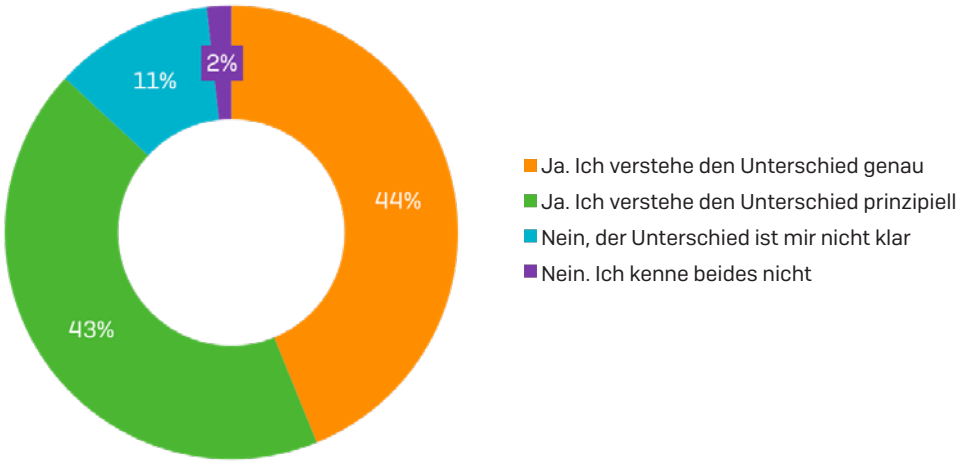
Ansicht der Befragten zur Aufnahme prädiktiver Technologien, wie etwa Machine und Deep Learning, zum Schutz vor komplexer Malware



Begriffliche Abgrenzung von Machine Learning und Deep Learning

Machine Learning ist momentan ein echtes Trendthema. Und dennoch gaben 56 % der Befragten an, dass sie den Unterschied zwischen Machine Learning und Deep Learning nur bedingt nachvollziehen können. Somit können sie die Sicherheitsoptionen im Angebot auch nicht uneingeschränkt bewerten.

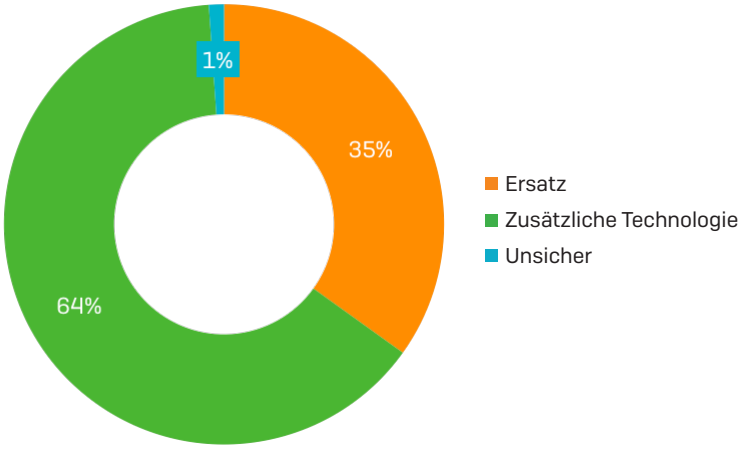
Fragen: Verstehen Sie den Unterschied zwischen Machine Learning und Deep Learning?



Machine Learning ist die Zukunft

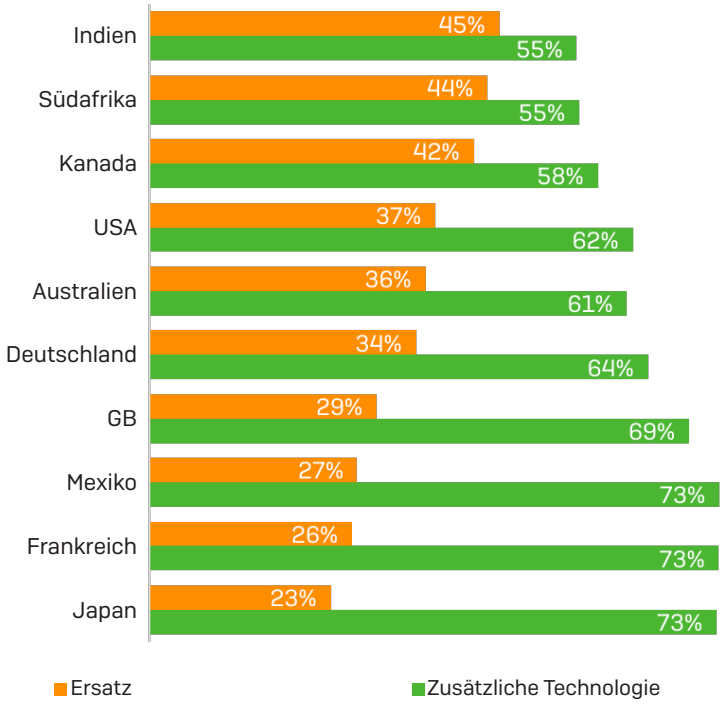
Wie wir bereits gesehen haben, nutzt die Mehrheit der befragten Unternehmen entweder bereits prädiktive Bedrohungsschutztechnologien, wie Machine Learning oder Deep Learning, oder planen eine Einführung der Technologien. Die Meinungen darüber, ob sich die Produkte in ihre Sicherheitsinfrastruktur einfügen, gehen jedoch auseinander. Beinahe zwei Drittel (64 %) der Unternehmen betrachten Machine und Deep Learning als Ergänzung ihrer Endpoint-Technologie an. 35 % hingegen sehen darin einen Ersatz für herkömmlichen Endpoint-Schutz.

Frage: Gelten Machine Learning und Deep Learning in Ihrem Unternehmen als zusätzlicher Endpoint-Schutz oder Ersatz für Antivirensoftware?



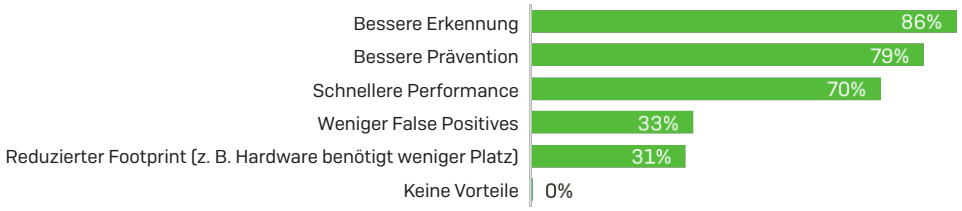
In indischen Unternehmen ist die Ansicht, dass die Technologien Virenschutzsoftware ablösen werden, mit 45 % am größten. Unter den japanischen Umfrageteilnehmern wurde die Technologie wiederum mit der größten Skepsis begegnet.

Frage: Gelten Machine Learning und Deep Learning in Ihrem Unternehmen als zusätzlicher Endpoint-Schutz oder Ersatz für Antivirensoftware?



Von Machine Learning und Deep Learning erhoffen sich 86 % der Unternehmen in erster Linie besseren Schutz.

Frage: Welche Vorteile erhofft sich Ihr Unternehmen vor allem von prädiktiven Technologien, wie Machine Learning und Deep Learning?



Beinahe zwei Drittel (65 %) hegen jedoch auch Bedenken über False Positives bei der Technologie.

Und dennoch ist die allgemeine Einstellung gegenüber Machine Learning sehr positiv: 94 % der Befragten sind der Ansicht, dass die Technologie zu Recht hochgejubelt wird. Immerhin 21 % erwarten sich hiervon sogar die Lösung sämtlicher Technologieprobleme.

	Durch-schnitt	GB	Frank-reich	Deutschland	USA	Kanada	Mexiko	Indien	Australien	Japan	Südafrika
Machine Learning wird zu Recht hochgejubelt	94 %	90 %	96 %	94 %	97 %	97 %	98 %	99 %	89 %	79 %	93 %
Machine Learning löst sämtliche Technologiepro-bleme	21 %	13 %	19 %	10 %	26 %	20 %	32 %	45 %	14 %	9 %	17 %

Ansicht der Befragten zu Machine Learning

Auch wenn sich die Befragten weitgehend einig sind, dass Machine Learning den Erwartungen gerecht wird, gehen die Meinungen darüber auseinander, ob es sich um ein Allheilmittel für unsere Technologieprobleme handelt. Wie bereits erwähnt, stehen IT-Manager in Indien der Technologie sehr positiv gegenüber. Ganze 45 % sind der Meinung, dass sich hierdurch all unsere Technologieprobleme lösen lassen. Jedoch teilen nur 9 % der japanischen und 10 % der deutschen Umfrageteilnehmer diese Auffassung.

Unsere Perspektive

Machine Learning wird zum Mainstream. Obwohl die Technologie relativ neu ist, plant die Mehrheit der Unternehmen bereits, sie in den nächsten 12 Monaten einzuführen. Wir stimmen der Mehrheit der Befragten zu: Machine Learning stellt eine zusätzliche Sicherheitsebene dar, kann jedoch Endpoint-Schutz nicht komplett ablösen.

Da die Unterschiede zwischen Machine Learning und Deep Learning für Viele nicht im Detail nachvollziehbar sind, muss die IT-Security-Branche dafür sorgen, dass Unternehmen fundierte Entscheidungen zu diesen Technologien treffen können. Dies lässt sich durch unabhängige, öffentliche Tests sowie Aufklärung über die Technologien sowie ihrer Abgrenzung erreichen.

Unsere Empfehlungen

Die Abwehr vor Malware gestaltet sich zunehmend komplexer. Zudem nutzen Cyberkriminelle Machine Learning bereits für ihre Angriffe. Sie müssen sicherstellen, dass Ihre IT-Sicherheit mit den Bedrohungen Schritt hält. Je schneller Machine Learning und Deep Learning angenommen werden, desto besser.

Wissenslücken müssen geschlossen werden: IT-Experten sollten sich die Zeit nehmen, sich intensiv mit Machine Learning und Deep Learning zu beschäftigen, um die Begriffe besser abgrenzen zu können und zu verstehen, wie sich die Unterschiede auf die IT-Sicherheit auswirken. Nicht alle Machine-Learning-Lösungen sind gleich. Stellen Sie sicher, dass Ihre IT-Security-Lösung den nötigen Schutz bietet.

Fazit

Die Umfrage verdeutlicht ganz klar, dass IT-Security für Unternehmen weltweit nach wie vor eine große Herausforderung darstellt, was nicht zuletzt an der zunehmenden Komplexität von Malware-Angriffen und dem finanziellen Anreiz für Cyberkriminelle liegt.

Die Kluft zwischen Know-how und Geschick der Angreifer, insbesondere bezüglich Ransomware und Exploits, und dem Wissen der IT-Experten, die mit ihrer Abwehr betraut sind, wächst. Dieser Vorsprung der Cyberkriminellen lässt sich jedoch durchaus durch Aufklärung und Information ausgleichen.

Aus der Umfrage geht klar hervor, dass herkömmliche Sicherheitslösungen Unternehmen nicht mehr hinreichenden Schutz vor den komplexen Bedrohungen von heute bieten. Das Angebot an Lösungen auf dem Markt ist groß. Da Unternehmen ihre Funktionsweise jedoch nicht immer uneingeschränkt nachvollziehen können, gestaltet sich auch die Auswertung und Implementierung des erforderlichen Schutzes schwierig.

Wir möchten an die Security-Branche appellieren, IT-Managern das Verständnis und die Bewertung dieser Technologien durch mehr öffentliche, unabhängige Tests sowie Aufklärung zu erleichtern.

Weiteres Informationsmaterial

- Exploits in der Falle – Ein lesenswerter Leitfaden zu Exploits, ihrer Funktionsweise sowie ihrer Abwehr
- Exploits unter der Lupe – Detaillierte Analyse von Hackern genutzter Exploits sowie von Schutzfunktionen zu ihrer Abwehr
- Die besten Tipps zum Schutz vor Ransomware – Die Funktionsweise von Ransomware und wie Sie sich davor schützen
- Machine Learning für Cybersecurity, entmystifiziert – Eine Zusammenstellung von Artikeln zum Thema Machine Learning
- Datenblatt zu Sophos Intercept X Deep Learning – Anschauliche Erklärung von Deep Learning und der Vorteile gegenüber Machine Learning

Jetzt neu: Sophos Intercept X

Sophos Intercept X ist der weltweit umfassendste Next-Gen-Endpoint-Schutz. Durch die Kombination aus einer Vielfalt an Technologien, wie Deep Learning, Ransomware Prevention sowie Anti-Exploit-Funktionen, schützt die Lösung vor Ransomware sowie bisher unbekannter Malware.

Intercept X lässt sich parallel zu Ihren Virenschutzprodukten von Sophos oder anderen Anbietern ausführen und bietet Ihnen zusätzlichen Schutz vor Ransomware und komplexen Angriffen. In der Kombination mit Sophos Endpoint Protection profitieren Sie von der branchenweit besten Abwehr von bekannten und neuen Bedrohungen.

Unabhängige Experten- und Kundenaussagen bestätigen die Effektivität von Intercept X:

„Intercept X hat jeden komplexen, hochentwickelten Angriff gestoppt, mit dem wir die Lösung konfrontiert haben“. ESG Labs

„Einer der besten Performance Scores, den wir jemals beobachten konnten.“ AV-TEST

Security Innovation of the Year
Computing Security Awards 2017

„Ransomware-Schutz mit Intercept X bietet uns einen massiven Mehrwert und erleichtert uns die notwendige Ausrichtung für die Zukunft der IT-Sicherheit enorm.“

Gus Garcia, Security and Information Officer, Diözese von Brooklyn

Nähere Informationen sowie Zugang auf unseren kostenlosen 30-Tage-Test erhalten Sie unter www.sophos.de/interceptx.

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

2.2.18 DE (GH)

SOPHOS