2022

ESET Cybersicherheits-Umfrage

DIE STIMMUNGSLAGE BEI KMUs.
WO DER SCHUH DRÜCKT.
WARUM EDR EINE LÖSUNG DARSTELLT.

Digital Security

Progress. Protected.

STATUS QUO

Werden KMUs auf Endpoint Detection und Response setzen, um so ein höheres Sicherheitsniveau zu erreichen?

Michal Jankech
Vice President of SMB and MSP Segment

"Im Business kommen die Probleme oft als Trio - oder sogar als Quartett. Denken Sie an das Bermuda-Dreieck, den mehrköpfigen Höllenhund Zerberus oder die vier apokalyptischen Reiter. Wenn Sie die digitale Sicherheit in einem kleinen oder mittelständischen Unternehmen verantworten, werden Sie früher oder später mit diesem Trio konfrontiert sein: Zu wenige Mitarbeiter, fehlendes Sicherheitsbewusstsein und mangelndes Verständnis der eigenen Verantwortung. Dies wirkt sich direkt auf das Budget und die Ressourcen aus. Und das vierte Problem? Sich verändernde soziale, politische oder ökonomische Rahmenbedingungen."

eset Digital Security
Progress. Protected.

NEW WORK UND DIGITALISIERUNGSSCHUB

Vor der COVID-19-Pandemie schienen die Technologiebranche, der Einzelhandel, die Telekommunikationsbranche und sogar die IT-Sicherheitsbranche verlässlich zu wachsen. In gleichem Maße schritt auch die Digitalisierung unauffällig voran. Neue Formen des Handels, der Kommunikation, der Dienstleistungen und Produkte hatten sich etabliert. Aber nur selten entfaltete die Digitalisierung ihr volles Potenzial. Dann kam COVID-19 und drückte den Fast-Forward-Knopf. Unternehmen rationalisierten ihre Prozesse und steigerten rasant ihre Produktivität. New Work und cloud-basierte Plattformen von Zoom bis Microsoft Teams etablierten sich im Arbeitsalltag der Mitarbeiter in kürzester Zeit. Die Digitalisierung nahm rapide an Fahrt auf.

IT-Budgets wuchsen drastisch und veränderten die Art und Weise, wie wir arbeiten, handeln und einkaufen. Parallel dazu schienen Sicherheitserwägungen einen neuen Trend bei kleinen und mittleren Unternehmen (KMU) auszulösen. Sie liebäugeln sowohl mit Cloud-Office-Sicherheit als auch mit fortschrittlicheren Erkennungs- und Reaktionstechnologien. Mahnende Beispiele gab es in den Jahren 2020 bis 2022 reichlich, wie etwa den Angriff auf den IT-Dienstleister Kaseya, Attacken auf Microsoft Exchange und die Emotet-Schadprogramme. Das alles geschieht in einer Reihe mit webbasierten Angriffen und der bereits realen Bedrohung durch Ransomware.

eset Digital Security
Progress. Protected.

WO DER SCHUH DRÜCKT

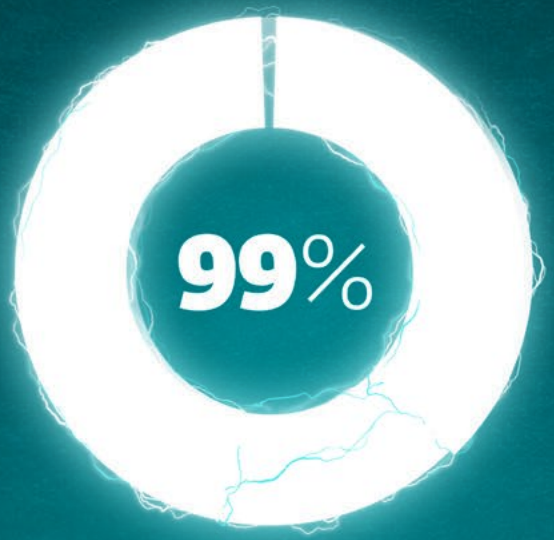
Inzwischen hat sich die Lage weiter zugespitzt: Über den Fachkräftemangel, die Chip-Knappheit und die Rezession hinaus tobt jetzt ein Krieg in der Ukraine, der weltumspannende Folgen mit sich bringt. Letzteren betrachten viele IT-Sicherheitsexperten als zusätzlichen Vektor für Cyberangriffe. Im Mittelpunkt der Berichterstattung stehen Bedrohungen, die sowohl auf Geschäftsschädigung als auch auf die Bewahrung nationalstaatlicher Interessen abzielen.

Obwohl alle Unternehmen mit diesen Herausforderungen in puncto IT-Security konfrontiert sind, müssen insbesondere KMUs lernen, ihr benötiges Schutzniveau zu definieren und entsprechend in Maßnahmen umzusetzen.

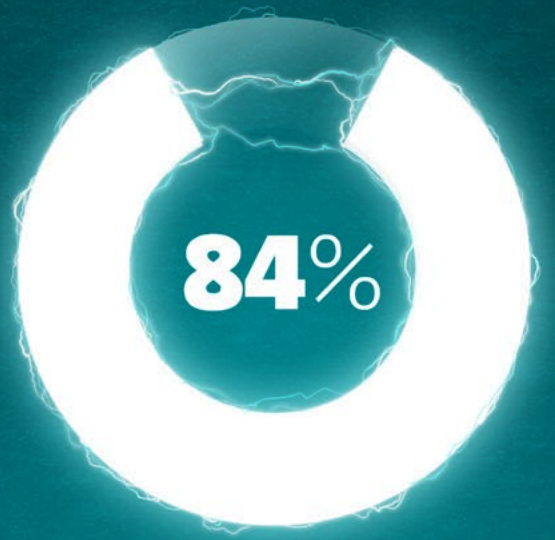
Genau diesen Punkt versucht die ESET Cybersicherheit-Umfrage in KMUs 2022 genauer zu beleuchten. Die Studie geht auch der Frage nach, wie kleine bis mittelständische Unternehmen die Lage in Hinblick auf personelle Ressourcen, technische Reife und finanzielle Belastung einschätzen.

eset Digital Security
Progress. Protected.

KMUs SIND DAS RÜCKGRAT DER WELTWIRTSCHAFT



aller Unternehmen in Europa und Nordamerika sind KMUs



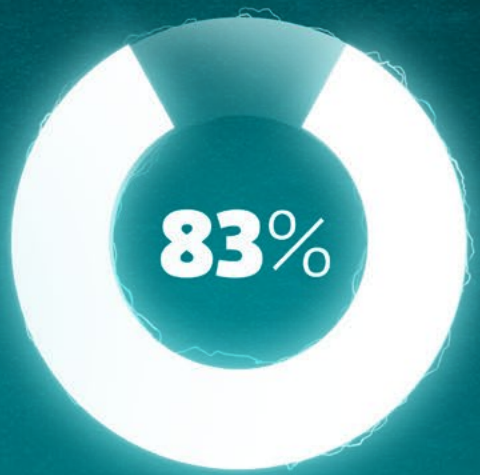
der KMUs versprechen sich Wachstum **durch technologischen Fortschritt**

 ESET Cybersicherheits-Umfrage 2022: Die Stimmungslage bei KMUs.

eset Digital Security
Progress. Protected.

DER ESET THREAT REPORT ZEIGT:
KMUs STEHEN VOR GROSSEN HERAUSFORDERUNGEN

20% Zunahme von Sicherheitsbedrohungen

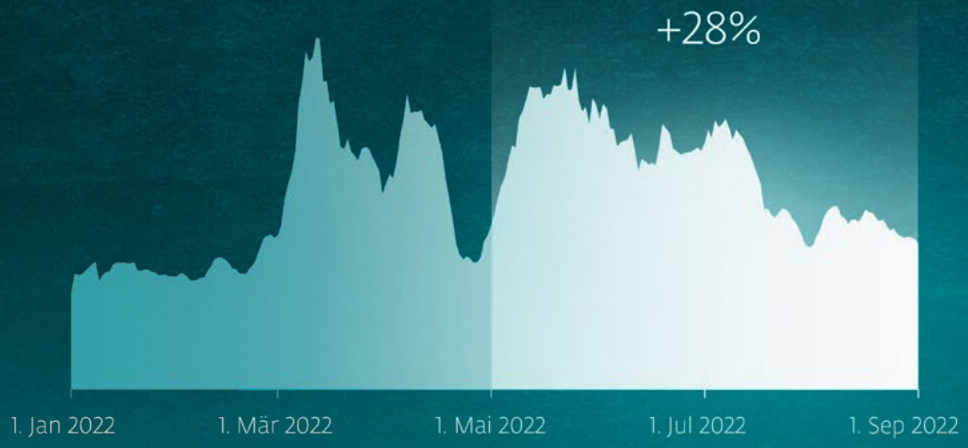


der KMUs sehen in Cyber-Kriegführung eine **höchst reale Bedrohung**, die jeden treffen kann

eset Digital Security
Progress. Protected.

KMUs ERWARTEN EINE FLUT AN WEB- UND E-MAIL-BEDROHUNGEN

E-Mail- und webbasierte Attacken zählen nach Einschätzung von ESET weiterhin zu den Top-Angriffsvektoren, denen Unternehmen ausgesetzt sind. Kleine und mittlere Unternehmen sollten sich bei der Abwehr von Cyberangriffen keinesfalls nur auf bekannte Einfallstore beschränken.



28% Anstieg der Web-Attacken

66% Anstieg von Phishing-E-Mails, die Outlook-Login-Daten stehlen wollen

ESET Cybersicherheits-Umfrage 2022: Die Stimmungslage bei KMUs.

eset Digital Security
Progress. Protected.

SO SCHÄTZEN KMUs DIE SECURITY-LAGE EIN

KMUs kennen sehr wohl die vielfältigen Risiken und Bedrohungen durch Cybercrime. Gleichzeitig haben sie wenig Vertrauen in ihre eigene Fähigkeit zur Gefahrenabwehr. Sie befürchten vorranig, Opfer von Malware oder webbasierten Attacken zu werden.

Erwartete Top-Bedrohungen in den nächsten 12 Monaten

 ESET Cybersicherheits-Umfrage 2022: Die Stimmungslage bei KMUs.

eset Digital Security
Progress. Protected.

SO SCHÄTZEN KMUs DIE SECURITY-LAGE EIN

Was ist der Grund für diese Bedenken? Es mag überraschen, dass kleine und mittlere Unternehmen das mangelnde Cyber-Sicherheitsbewusstsein ihrer Mitarbeiter als Hauptproblem sehen – und das sogar vor Faktoren wie den Auswirkungen des Ukraine-Kriegs und dem anhaltenden Trend zum Remote-Arbeitsplatz. Beides hat bei vielen KMUs zu erhöhten Investitionen in die Cybersicherheit geführt.

Top-5-Schwachstellen aus Sicht von KMUs

43%
Mangelndes Cyber-**Sicherheitsbewusstsein** der Mitarbeiter

37%
Angriffe von **staatlichen Akteuren** aufgrund des Ukraine-Kriegs

34%
Schwachstellen **bei Partnern und Lieferketten**

32%
fortgesetzte Hybrid- oder **Remote-Arbeit**

31%
Nutzung des **Remote Desktop Protocol (RDP)**

ESET Cybersicherheits-Umfrage 2022: Die Stimmungslage bei KMUs.

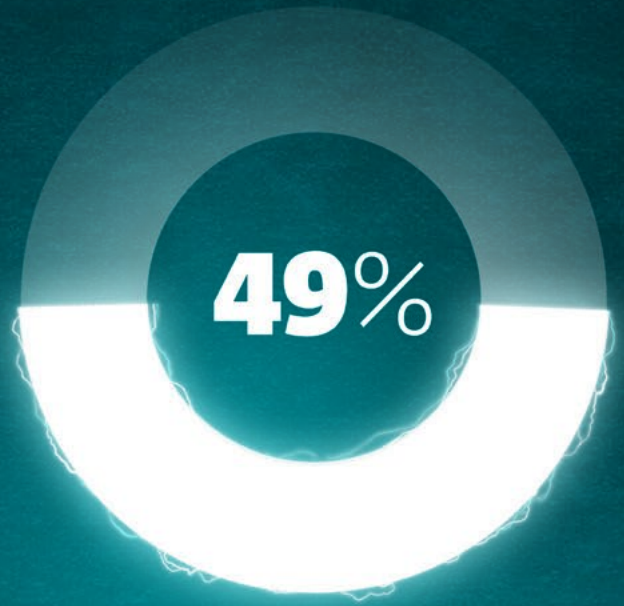
eset Digital Security
Progress. Protected.

SO SCHÄTZEN KMUs DIE SECURITY-LAGE EIN

Auf jeden Fall erkennen KMUs Handlungsbedarf. Die größten Herausforderungen bestehen derzeit darin, mit der rasanten Entwicklung der Cybersicherheits-Bedrohungen Schritt zu halten und die erforderlichen Sicherheitsmechanismen zu implementieren. Grundlegende Voraussetzung dafür – und gleich die nächste Herausforderung – ist das erforderliche Budget.

Wie werden Unternehmen angesichts der wirtschaftlichen Veränderungen durch COVID-19 und dem anhaltenden Krieg in Europa ihre Prioritäten setzen?

Denn auch Unternehmen, die oberflächlich betrachtet die Investition in Cybersicherheits-maßnahmen sparen, können später mit hohen Kosten durch einen Sicherheitsvorfall konfrontiert werden.

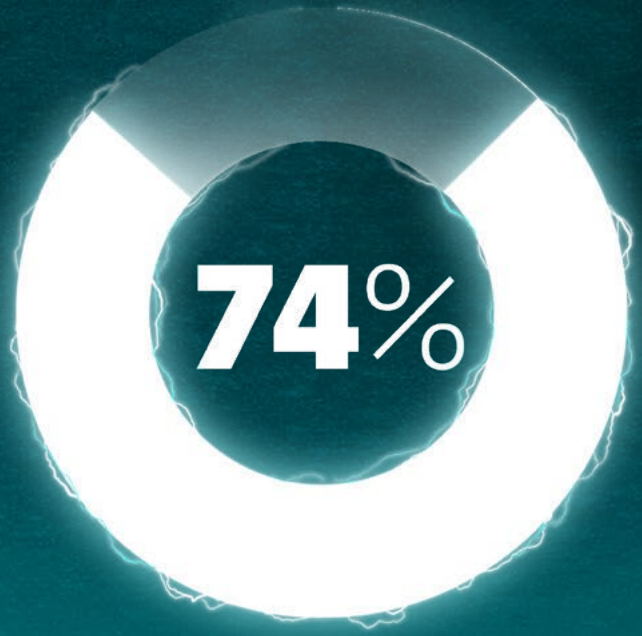


Budgetbeschränkungen / fehlende Investitionen in die Cybersicherheit gehören zu den drei größten Herausforderungen für IT-Abteilungen kleiner und mittlerer Unternehmen

eset Digital Security
Progress. Protected.

KMUs FÜHLEN SICH VERLETZLICHER ALS GROSSUNTERNEHMEN

Über alle Unternehmensgrößen hinweg betrachten sich **74 Prozent der kleinen und mittelständischen Unternehmen** aufgrund ihrer Größe anfälliger für Cyberattacken als Großunternehmen und Konzerne.

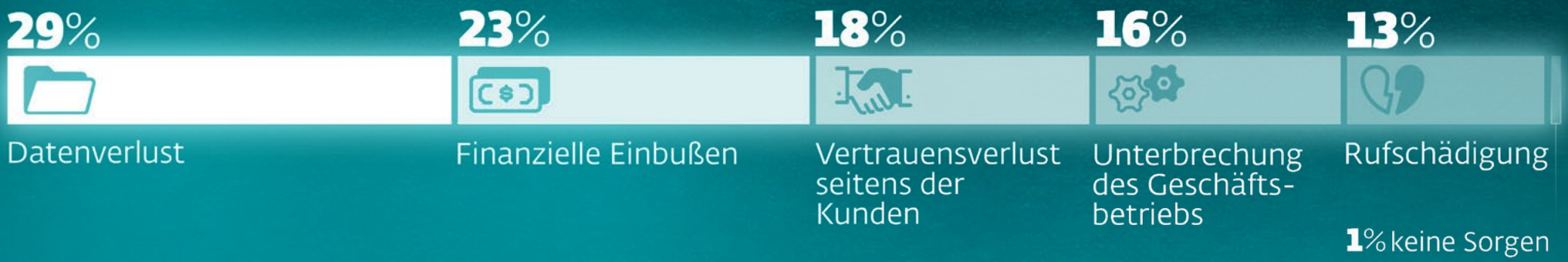


eset Digital Security
Progress. Protected.

KMUs FÜHLEN SICH VERLETZLICHER ALS GROSSUNTERNEHMEN

Insbesondere KMUs sehen die größten Risiken in Vorfällen, die zu Datenverlusten oder schwerwiegenden finanziellen Einbußen führen. Im vergangenen Jahr waren zwei Drittel der Befragten von einem Datensicherheitsvorfall betroffen. Dessen Untersuchung dauerte in den meisten Fällen bis zu drei Monate. Die geschätzten Gesamtkosten beliefen sich im Durchschnitt auf fast 220.000 Euro.

Das sind die größten Ängste vor den Folgen eines Cyberangriffs

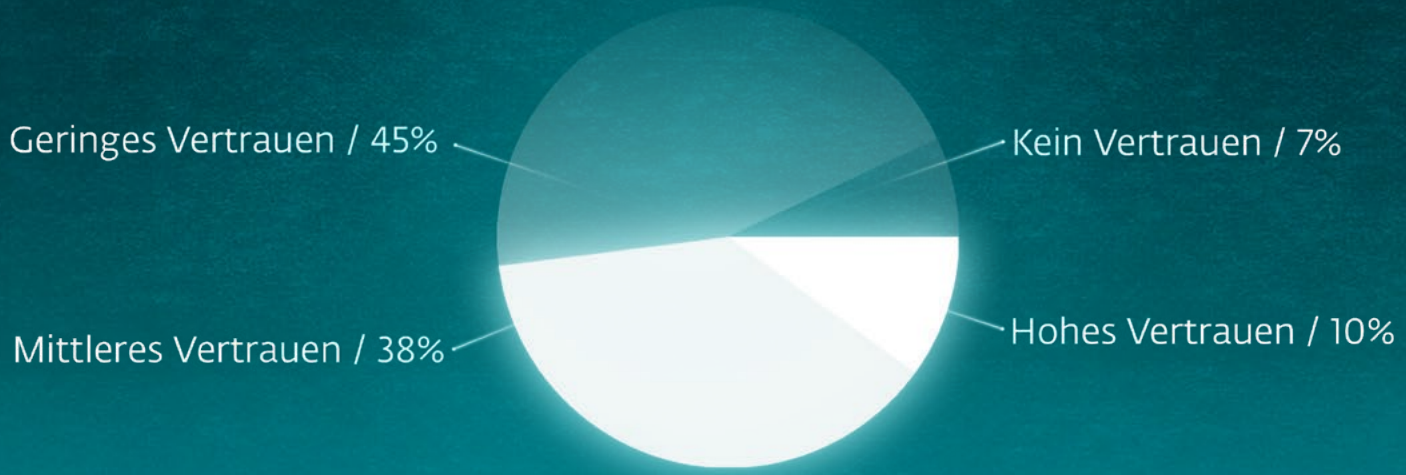


eset Digital Security Progress. Protected.

WENIG VERTRAUEN
IN DIE EIGENE CYBER-ABWEHR

Es überrascht, dass lediglich 10 Prozent der befragten Unternehmen ein hohes Vertrauen in die eigene Cyber-Resilienz besitzen. Unsicherheitsfaktoren sind vor allem der interne Wissenstand beim Thema Internetsicherheit, der Zugang zu externen Experten und unzureichende Reaktionszeiten bei Vorfällen.

Vertrauen in die Cyber-Resilienz in den nächsten 12 Monaten



Nur **48% der KMUs** gaben an, ein mittleres / hohes Vertrauen in ihre Cyber-Resilienz zu haben

eset Digital Security
Progress. Protected.

WENIG VERTRAUEN
IN DIE EIGENE CYBER-ABWEHR

Fragt man nach komplexen IT-Sicherheitsprozessen, haben 71 Prozent der Unternehmen sehr großes Vertrauen. EDR-Produkte kommen lediglich bei jedem dritten KMU zum Einsatz. Dieser Unterschied deutet entweder auf übermäßiges Vertrauen in die aktuellen Sicherheitsmaßnahmen hin. Oder es nährt den Verdacht, dass das Verständnis für Endpoint Detection and Response im Allgemeinen und dessen Vorteile im Speziellen deutliche Lücken aufweist.

Sind KMUs wirklich gut aufgestellt?

32%
vertrauen den
Cybersecurity-Kenntnissen
ihres IT-Teams

30%
sind mit der
Geschwindigkeit zufrieden,
mit der Bedrohungen erkannt
und isoliert werden und
wie darauf reagiert wird

27%
sprechen ihren
IT-Teams große
Fähigkeiten
in der Forensik zu

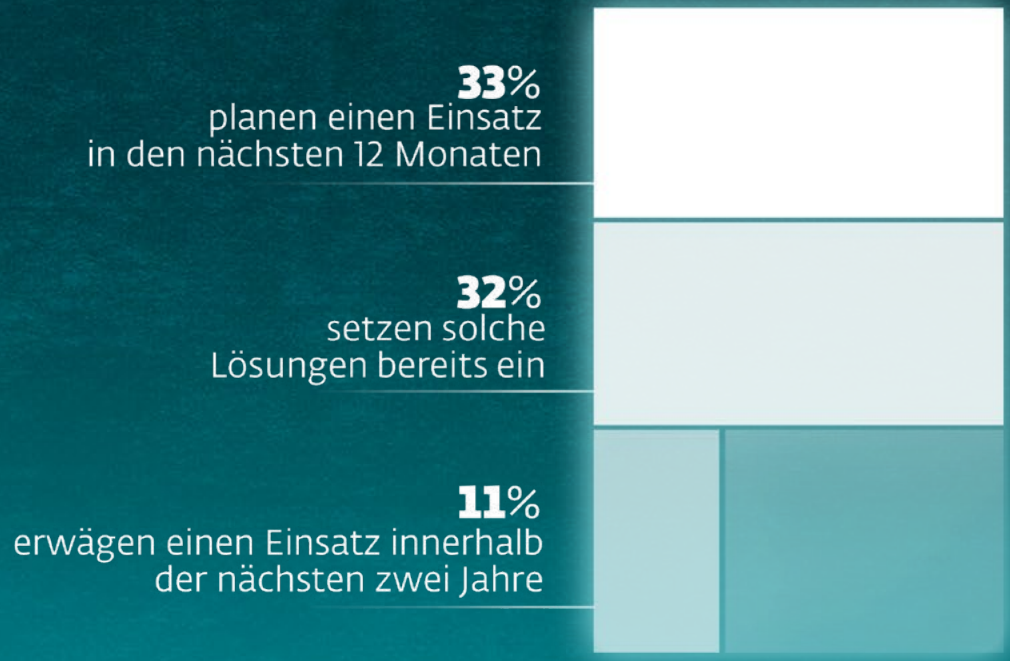
eset® Digital Security
Progress. Protected.

DER BEDARF AN EDR WÄCHST

Die typische Reaktion auf Cybersicherheitsvorfälle: Unternehmen investieren zuerst in die Schulung des IT-Teams. Das überrascht auf den ersten Blick nicht, löst aber das eigentliche Problem nicht im erforderlichen Maße. Oftmals mangelt es an der Balance zwischen notwendiger Technologie, vorhandener Cyber-Security-Architektur und Mitarbeiterschulung.

Der Einsatz von Endpoint Detection und Response Lösungen ist nicht flächendeckend (lediglich 32% der befragten Unternehmen setzen diese ein), aber die gute Nachrichtist: Jedes dritte der befragten KMU will hier nachbessern und das Schutzniveau deutlich verbessern.

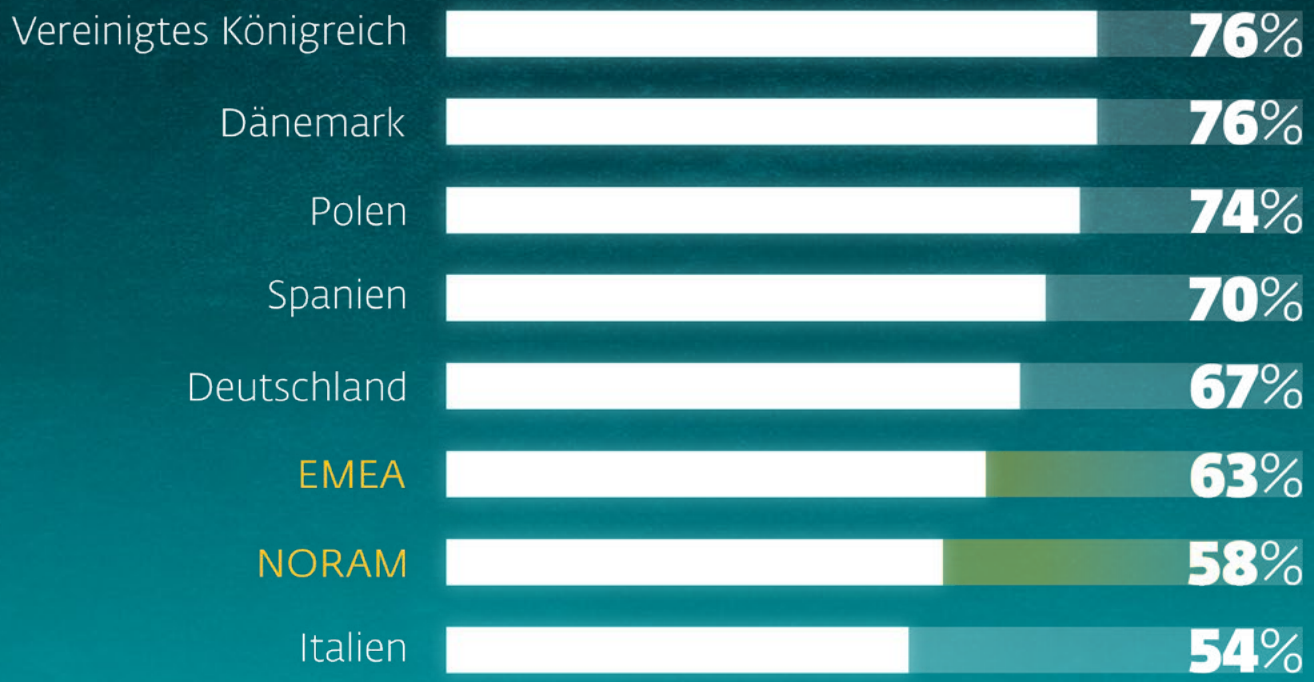
Nutzung von EDR / XDR / MDR Lösungen



eset Digital Security
Progress. Protected.

IM SCHNELLEN, WEILTWEITEN VERGLEICH HAT EUROPA DIE NASE VORN

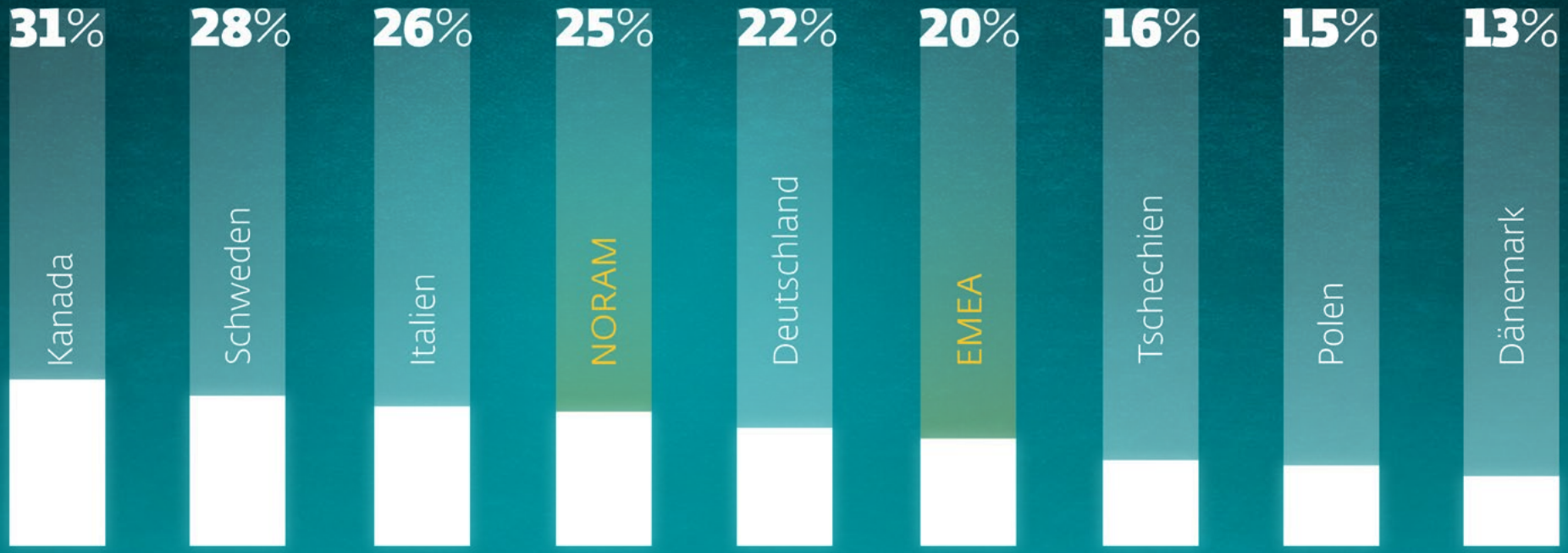
Das Thema EDR scheint in Europa populärer oder schneller im IT-Alltag angekommen zu sein als in Nordamerika. In EMEA gaben 67 Prozent der Befragten an, EDR bereits zu nutzen oder in den nächsten 12 Monaten zu implementieren. In den NORAM-Staaten liegt der Wert bei lediglich 58 Prozent. Nur in einem europäischen Land (Italien, 54%) ist EDR etwas weniger verbreitet. Spitzenreiter sind das Vereinigte Königreich und Dänemark (76%), Polen (74%) und Spanien (70%). Deutschland rangiert mit 67 Prozent im unteren Mittelfeld.



eset Digital Security Progress. Protected.

NACHHOLBEDARF IN PUNCTO WISSEN
UM ENDPOINT DETECTION AND RESPONSE

Auch wenn die zuvor genannten Zahlen ein positives Bild zeichnen, ist das Thema Endpoint Detection and Response noch längst nicht in allen Köpfen präsent. Auf die Frage, ob man mit dem Thema EDR vertraut sei, antworteten in der Spitze 31 Prozent der Befragten (Kanada), dass das vorhandene Wissen nicht ausreiche, um eine Entscheidung für solche Lösungen treffen zu können. In EMEA gab dies jeder Fünfte, in Nordamerika sogar jeder Vierte an. Große Unterschiede zeigten sich gerade in den EMEA-Ländern: Während Dänemark (13%), Polen (15%) und Tschechien (16%) mit vergleichsweise niedrigen Werten glänzten, haben Schweden (28%) und Italien (26%) Nachholbedarf. Deutschland positioniert sich mit 22 Prozent erneut im Mittelfeld.



eset Digital Security
Progress. Protected.

SO ARBEITET
ENDPOINT DETECTION AND RESPONSE

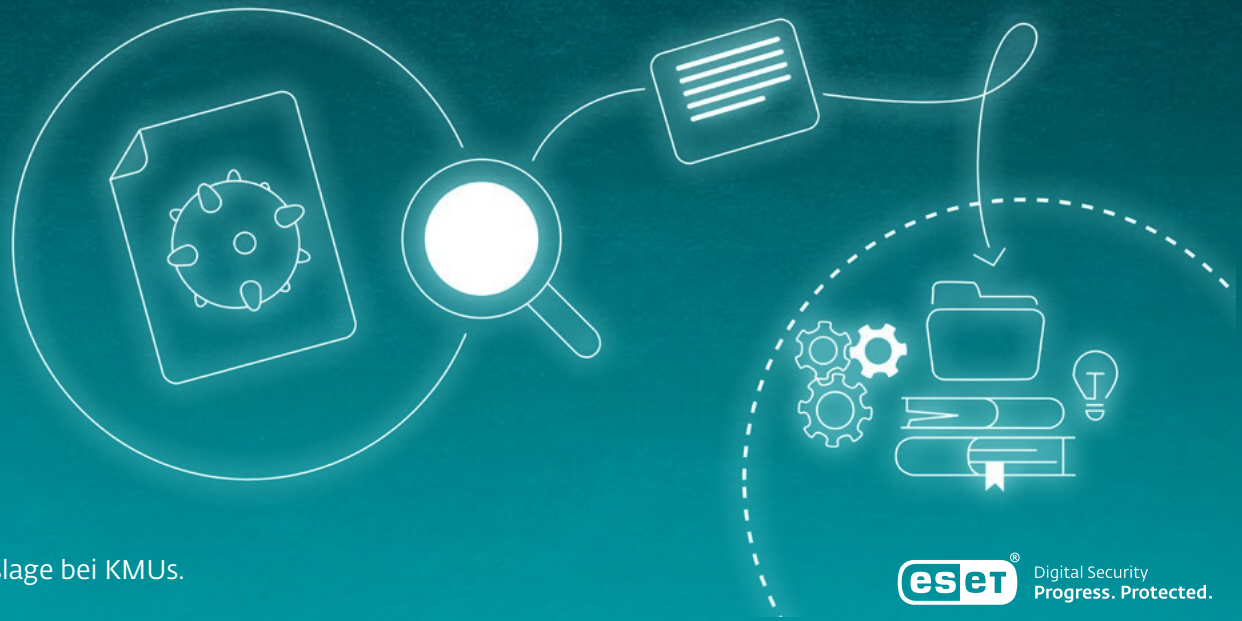
Endpoint Detection and Response-Lösungen erhöhen das Schutzniveau von Unternehmen deutlich und ermöglichen IT-Security-Verantwortlichen eine umfassende Innensicht ihres Netzwerks. Aber was bedeutet Detection und Response eigentlich in der Praxis? Zum einen soll damit der Endpoint geschützt werden („Detection"), auf dem die meisten Hacker-Aktivitäten stattfinden. Dort liegt ein Großteil der schutzwürdigen Daten vor beziehungsweise werden am Gerät zum Beispiel Passwörter oder Bankdaten eingegeben. Zum anderen beschreibt „Response", dass auf Anomalien sofort reagiert werden kann.

Alle Aktivitäten innerhalb der IT-Infrastruktur (Nutzer-, Datei-, Prozess-, Registry-, Speicher- und Netzwerkvorgänge) können dank EDR in Echtzeit überwacht und bewertet werden. Bei Bedarf kann der IT-Verantwortliche sofort manuell handeln oder es greifen automatische, zuvor definierte Verhaltensweisen ein. Nur auf diese Weise lassen sich erste Spuren von Hackern identifizieren, Fehlverhalten von Mitarbeitenden bestimmen und Sicherheitsmängel ausfindig machen. Oder die Einfallstore finden, die bei einem erfolgreichen Hackerangriff auf das eigene Netzwerk zu weit offenstanden.

IT-FORENSIK KOMMT HACKERN AUF DIE SPUR

Die Auswertung aller Endpoint-Daten in einem Netzwerk lässt Rückschlüsse auf die Validität einzelner Abläufe zu. Eine genaue Erfassung von alltäglichen Vorgängen wie das Kopieren von Dateien, User-Zugriffe auf bestimmte Bereiche im Netzwerk, aber auch An- und Abmeldungen von Anwendern erlaubt bei entsprechender Auswertung ein Herausfiltern bösartiger Aktivitäten.

Zudem bieten Endpoint- und Response-Lösungen eine weitere wichtige Einsatzmöglichkeit: Mit ihrer Hilfe können nach einer Cyberattacke forensische Untersuchungen vorgenommen werden. Ähnlich einem Mordfall in bekannten Krimis werden möglichst viele Informationen gesammelt und Alibis, in diesen Fällen die ordnungsgemäßen Arbeitsweisen, überprüft. Administratoren erkennen dann zuverlässig, wie der Angriff ablief, welche Schwachstellen konkret ausgenutzt und welche Veränderungen im Netzwerk vorgenommen wurden.



eset Digital Security
Progress. Protected.

NACHHOLBEDARF IST ERKENNBAR

Es gleicht dem bekannten Henne-Ei-Problem: KMUs erkennen zwar den Wert ganzheitlicher IT-Sicherheitskonzepte, aber beim Einsatz der hierfür erforderlichen Technologien ist Nachholbedarf erkennbar. Nur 32 Prozent der kleinen bis mittleren Unternehmen nutzen demnach EDR-Lösungen. Ebenso gilt es aber, das Know-how und die personelle Ausstattung der hierfür verantwortlichen Akteure weiter auszubauen.

Fazit: *Die ESET Cybersicherheits-Umfrage in KMUs 2022* zeigt die Notwendigkeit einer effektiven Strategie, die Lücken schließt und die Cyber-Resilienz stärkt. Mit einem intelligenten und skalierbaren Einsatz von Endpoint Detection and Response kann Ihr Unternehmen die Widerstandsfähigkeit in der Tat erhöhen. Und Sie können sich wieder auf Ihre Kernkompetenzen, Ihr Wachstum und Ihre Innovation konzentrieren.

Wir denken, dass dieser Bericht die aktuelle Stimmung in KMUs eindrücklich widerspiegelt. Und er zeigt, welche Schwachstellen es schnell zu beseitigen gilt.

eset® Digital Security
Progress. Protected.

ESET und das unabhängige britische Marktforschungs-Institut Insight Avenue haben die *ESET Cybersicherheits-Umfrage 2022* in enger Zusammenarbeit erstellt. Es wurden 1.212 IT-Sicherheits-Entscheider aus England, den USA, Kanada, Frankreich, Spanien, Italien, Polen, Schweden, Tschechien, den Niederlanden, Dänemark, Norwegen und Finnland interviewt. Die Befragten repräsentieren Unternehmen mit einer Größe von 25 bis 500 Mitarbeitern sowie in puncto IT-Sicherheitsprozesse mit unterschiedlichen Reifegraden und Budgets.

Medienkontakt: **presse@eset.de**