cybereason

UNTERNEHMEN IN GEFAHR

Ransomware-Angreifer machen keinen Urlaub

EINLEITUNG

CEO Insight

Die Urlaubszeit ist immer eine kritische Phase für Unternehmen, aber gerade in diesem Jahr gibt es eine Reihe von Faktoren, die diese noch herausfordernder gestalten als bisher. Die Welt setzt sich nach wie vor mit der COVID-19 Pandemie auseinander, Ladenregale sind leer, die Produktion im Verzug, Lieferketten sind blockiert und Personalengpässe führen zu Flugannullierungen.

Organisationen stehen außerdem vor einer weiteren Herausforderung. Erpressungs-Software (Ransomware) ist eine ernstzunehmende und wachsende weltweite Bedrohung. Nach der Hochrechnung eines Gutachtens werden die weltweiten Kosten für Cyberkriminalität 2021 die Marke von 6 Billionen US$ übertreffen. Das ist doppelt so viel wie noch vor 5 Jahren, und ein Großteil dieser finanziellen Auswirkungen ist auf Ransomware zurückzuführen.

Daher stellt sich die Frage, wie gut Unternehmen die Risiken von Ransomware-Attacken einschätzen können – vor allem jene, die an Wochenenden und in Urlaubszeiten auftreten – und wie gut sie darauf vorbereitet sind, dieser Gefahr entgegenzuwirken.

Es gab in 2021
ÜBER 200
Ransomware-Attacken, die Schlagzeilen machten

URLAUBS-GEFAHR RANSOMWARE

Ransomware ist eine tägliche Bedrohung, aber der Trend zeigt, dass die meisten Attacken an Wochenenden und in Urlaubszeiten stattfinden. Dann nämlich, wenn weniger Personal bereit steht, um die Attacken zu entdecken und darauf zu reagieren, weil die Mehrheit des Security Teams mit Familie und Freunden entspannen will. Der Colonial-Pipeline-Angriff fand z. B. am Muttertags-Wochenende statt. JBS wurde am amerikanischen Memorial-Day-Wochenende angegriffen. Die Kaseya Attacke passierte am amerikanischen Unabhängigkeitstag-Wochenende. Und die Liste lässt sich fortsetzen.

Tatsächlich gab es in 2021 bisher über 200 Ransomware-Angriffe, die Schlagzeilen machten – und dies sind nur die Attacken, die offiziell bekannt wurden. Technik-Giganten wie Acer und Apple waren jeweils von Erpressungsversuchen i. H. v. 50 Millionen US$ betroffen, und die Colonial- und JBS-Angriffe hatten kritische Auswirkungen auf die Lieferketten-Infrastruktur in den USA und störten damit empfindlich die gesamte Wirtschaft. Trotzdem alle Branchen bedroht sind, stellt die anstehende Urlaubszeit vor allem Einzelhandel und Transport in punkto Umsatzeinbußen und Lieferkettenstörungen vor hohe Anforderungen. Beide sind Faktoren, die Ransomware-Angreifer am wahrscheinlichsten als ihre Angriffsziele wählen, um ein möglichst hohes Lösegeld zu erpressen.

Verbunden mit der Tatsache, dass das durchschnittliche Lösegeld gegenüber 2020 mit 5,3 Millionen US$ um mehr als 500 % stieg und 83 % der betroffenen Unternehmen letztlich ein Lösegeld zahlten, ist offensichtlich, dass es sich um eine anhaltende Gefahr handelt. Noch alarmierender ist jedoch, dass 80 % aller Unternehmen, die ein Lösegeld zahlten, von einer weiteren Attacke betroffen waren.

Diese Studie zeigt die Tatsache auf, dass die Einschätzung, Entschärfung und Behebung eines Angriffs und die anschließende Wiederherstellung länger brauchen, wenn die Attacke am Wochenende oder in der Urlaubszeit erfolgt – ein gegnerischer Vorteil, dessen Angreifer sich sehr bewusst sind. Cybereason kooperiert mit Verteidigern, um diesen gegnerischen Vorteil ins Gegenteil zu verkehren. Dieser Bericht bietet Einsichten in das Risiko und Anleitung zu dessen Minimierung, damit abwehrende Unternehmen besser auf bevorstehende Ransomware-Attacken in der kommenden Urlaubssaison vorbereitet sind.

LIOR DIV
CEO, CYBEREASON

EIN KARTENHAUS

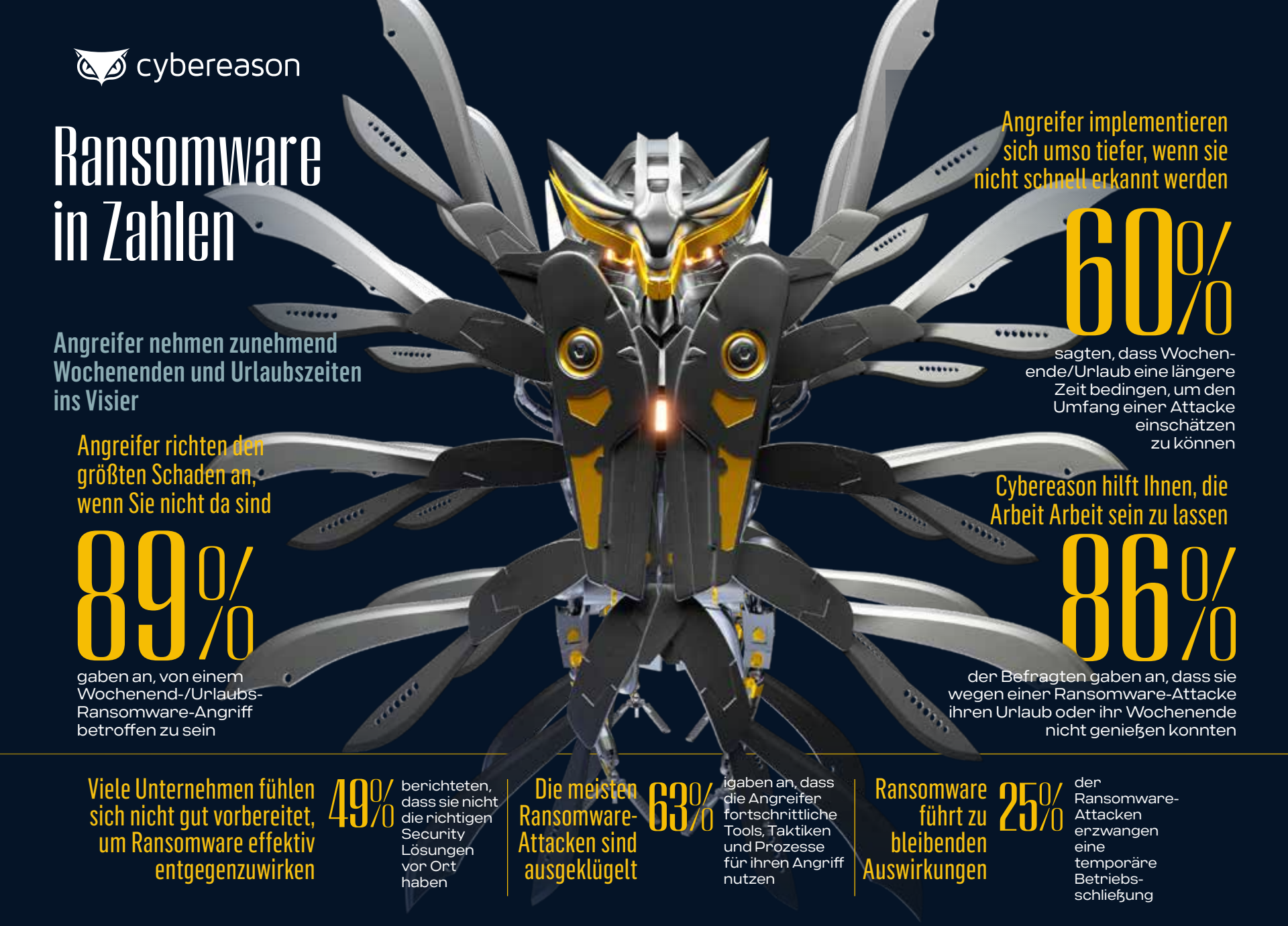
Stress und Burnout sind sehr reale Herausforderungen für Cybersecurity Experten. Security Teams sind unterbesetzt und überfordert in ihrem Bemühen, eine immer komplexere Angriffsfläche vor einer kontinuierlich wachsenden Bedrohungsumgebung zu schützen. Dabei müssen sie oft veraltete Tools nutzen, die moderne Bedrohungen weder erkennen noch beenden können.

Die Kombination einer schwachen Wirtschaft, die mit ihrer Lieferkettenlogistik kämpft , und der Wahrscheinlichkeit eines erheblichen Angriffs während der anstehenden Urlaubszeit erzeugt das Szenario eines Kartenhauses, das zusammenbrechen könnte, wenn etwas gegen den sprichwörtlichen Tisch stößt.

Wenn eine erhebliche Ransomware-Attacke während der kommenden Ferien erfolgt, könnte dies verheerende Konsequenzen haben für Unternehmen, die davon überrascht werden. Cybereason führte diese Studie durch, um Erkenntnisse zur **Abweichung des wahrgenommenen Risikos gegenüber der tatsächlichen Gefahr von Wochenend- und Urlaubs-Ransomware-Attacken für Unternehmen** aufzuzeigen.

cybereason

Ransomware in Zahlen



Angreifer nehmen zunehmend Wochenenden und Urlaubszeiten ins Visier

Angreifer richten den größten Schaden an, wenn Sie nicht da sind

89%

gaben an, von einem Wochenend-/Urlaubs-Ransomware-Angriff betroffen zu sein

Angreifer implementieren sich umso tiefer, wenn sie nicht schnell erkannt werden

60%

sagten, dass Wochenende/Urlaub eine längere Zeit bedingen, um den Umfang einer Attacke einschätzen zu können

Cybereason hilft Ihnen, die Arbeit Arbeit sein zu lassen

86%

der Befragten gaben an, dass sie wegen einer Ransomware-Attacke ihren Urlaub oder ihr Wochenende nicht genießen konnten

Viele Unternehmen fühlen sich nicht gut vorbereitet, um Ransomware effektiv entgegenzuwirken

49% berichteten, dass sie nicht die richtigen Security Lösungen vor Ort haben

Die meisten Ransomware-Attacken sind ausgeklügelt

63% igaben an, dass die Angreifer fortschrittliche Tools, Taktiken und Prozesse für ihren Angriff nutzen

Ransomware führt zu bleibenden Auswirkungen

25% der Ransomware-Attacken erzwangen eine temporäre Betriebsschließung

Wenn sich das Jahr seinem Ende nähert,

wechseln Unternehmen und Kunden in den Urlaubsmodus. Die Ferienzeit lässt Milliarden Dollar in die Wirtschaft fließen, weil Menschen Geschenke kaufen, sie an Feiertagsevents teilnehmen oder sie veranstalten, sie reisen, um Zeit mit ihrer Familie und Freunden zu verbringen – alles, um auf das vergangene Jahr zurückzuschauen und sich auf einen guten Start ins neue Jahr vorzubereiten.

Leider wechseln Cyberkriminelle ebenso in den Urlaubsmodus. Cybereason führte eine weltweite Forschungsstudie durch, um das tatsächliche Risiko von Ransomware-Attacken während Urlaubszeiten und Wochenenden besser einschätzen zu können.

Die Erkenntnisse dieser Studie unterstützen Verteidiger in ihrem Handeln und Unternehmen dabei, Prozesse und Tools vor Ort zu implementieren, um die Angriffe zu erkennen und zu beenden.

> Dieser November/Dezember wird besonders heftig werden, weil einige Menschen die Möglichkeit haben, das erste Mal seit Beginn der Pandemie ihre Familien wiederzusehen. Das bedeutet, dass Menschen weiter vom Büro entfernt sind und weniger wahrscheinlich Alarmmeldungen kontrollieren.

ANDREW
SECURITY ANALYST
RECHTSSEKTOR

Komplexe RansomOps

Erfolgreiche RansomOps ist ein Begriff, der die komplexeren Ransomware-Operationen, die heute vorherrschen, am besten beschreibt. Diese werden schleichend eingesetzt und sind ähnlich den APT-Taktiken so konstruiert, dass sie das anvisierte Netzwerk so umfangreich wie möglich infizieren, um immer höhere Lösegelder erpressen zu können – von denen einige bereits die 50-Millionen-US$-Marke überschreiten.

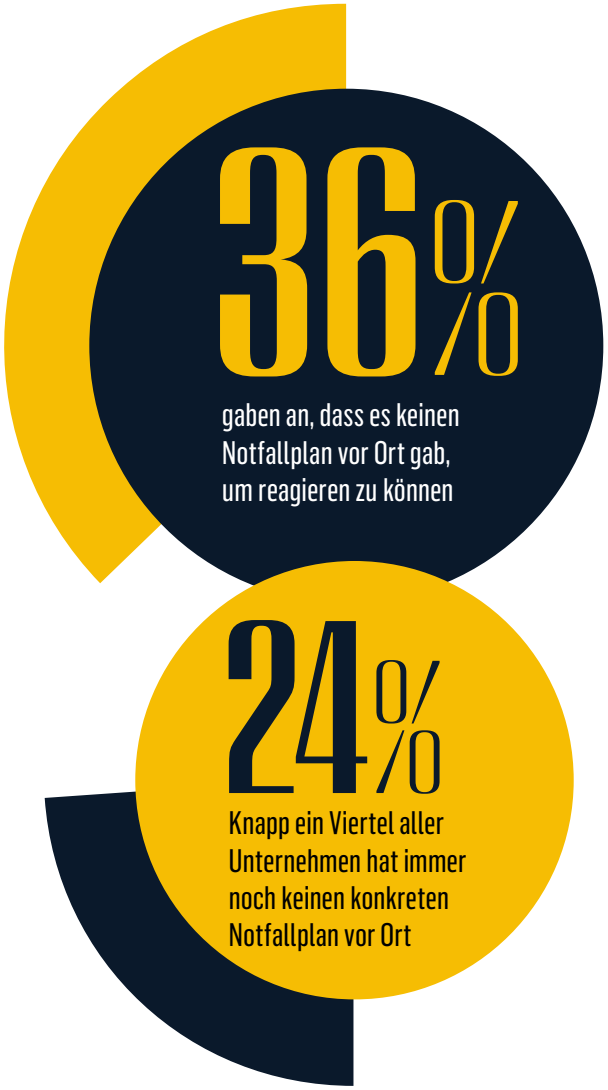
Am wichtigsten ist, über RansomOps zu wissen, dass die Angreifer bereits viele Wochen oder gar Monate vor der tatsächlichen, schädlichen Implementierung der Ransomware nachweisbare Aktivitäten im anvisierten Netzwerk unternahmen.

Hier setzen Strategien zur frühen Erkennung und Störung der RansomOps an, um ihre Kill Chain, die zu einem möglicherweise verheerenden Ransomware-Sicherheitsereignis führen könnte, in einen weniger schädlichen Eingriff und/oder Datenexfiltrationsversuch umzukehren.

WAHRNEHMUNG VS. REALITÄT:

Sind Unternehmen vorbereitet?

Im Juni 2021 veröffentlichte Cybereason den Report einer weltweiten Studie mit dem Titel Ransomware: Die wirklichen Kosten für Unternehmen, die gezeigt hat, dass die große Mehrheit der Unternehmen, die von einer Ransomware-Attacke getroffen wurden, im Ergebnis erhebliche Auswirkungen auf Ihren Geschäftsbetrieb erfahren mussten.



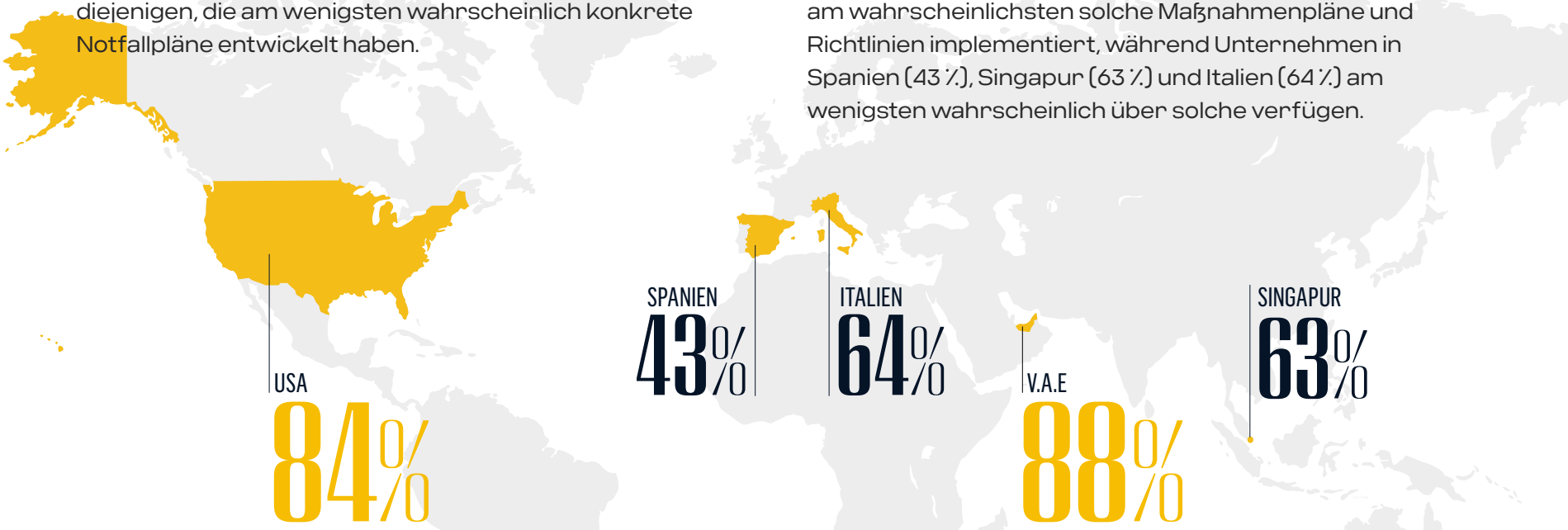
Die aktuelle Ransomware-Urlaubszeit-Studie betrachtete gezielt die Auswirkungen von Ransomware-Attacken, die darauf konzentriert waren, Unternehmen anzugreifen, wenn sie bezogen auf eine mögliche erfolgreiche Abwehr am meisten gefährdet waren: Wochenenden und Urlaubszeiten. Alle Studienteilnehmer arbeiteten in Unternehmen, die bereits Ziel eines Ransomware-Angriffs waren.

Trotzdem sie bereits Opfer waren – neben der Flut von veröffentlichten und extrem zerstörerischen Ransomware-Attacken, die 2021 an Wochenenden und in Urlaubszeiten stattfanden und Colonial Pipeline, JBS Meat Packers, Managed Services Provider Kaseya und weitere Unternehmen lahmlegten – **gaben mehr als ein Drittel (36 %) an, dass es keinen konkreten Notfallplan in ihrem Unternehmen gab, der ermöglicht hätte, auf die erlittene Ransomware-Attacke zu reagieren**.

Die Studie zeigte außerdem, dass **knapp ein Viertel (24 %) der Unternehmen immer noch keinen konkreten Notfallplan vor Ort hat,** obwohl sie bereits erfolgreich angegriffen wurden.

Die Studie zeigte auf, dass die Branchen Bau/Konstruktion (81 %) und IT/Telekommunikation (84 %) am wahrscheinlichsten gegen Ransomware-Attacken an Wochenenden/Urlaubszeiten vorbereitet sind. Demgegenüber sind die Branchen Gesundheit (65 %) und Produktion (67 %) – wohl zwei der größten Zielbranchen von Ransomware-Angriffen wegen ihres Potenzials für signifikante Umsatzverluste oder den Verlust von Menschenleben – innerhalb der Branchen diejenigen, die am wenigsten wahrscheinlich konkrete Notfallpläne entwickelt haben.

Ähnlich verhält es sich mit Unternehmen mit mehr als 2.000 Mitarbeitern – wobei die Unternehmensgröße häufig einen Zielfaktor für Angreifer bildet, um höhere Erpressungsgelder zu begünstigen – die mit knapp über zwei Dritteln (69 %) ebenfalls signifikant unterdurchschnittlich vertreten sind, wenn es um konkrete Notfallpläne oder Richtlinien vor Ort geht. Unternehmen in den USA (84 %) und den VAE (88 %) haben am wahrscheinlichsten solche Maßnahmenpläne und Richtlinien implementiert, während Unternehmen in Spanien (43 %), Singapur (63 %) und Italien (64 %) am wenigsten wahrscheinlich über solche verfügen.



Die Prozentzahlen zeigen die Unternehmen je Land, von denen angenommen wird, dass sie über konkrete Notfallpläne und Richtlinien verfügen.

20%

Ein Fünftel (20 %) glaubte, dass ihr Unternehmen niemals Ziel einer Ransomware-Attacke sein würde

63%

Zwei Drittel glaubten, dass die Angreifer komplexe staatliche Bedroher waren (APT/Fortgeschrittene, anhaltende Bedrohung)

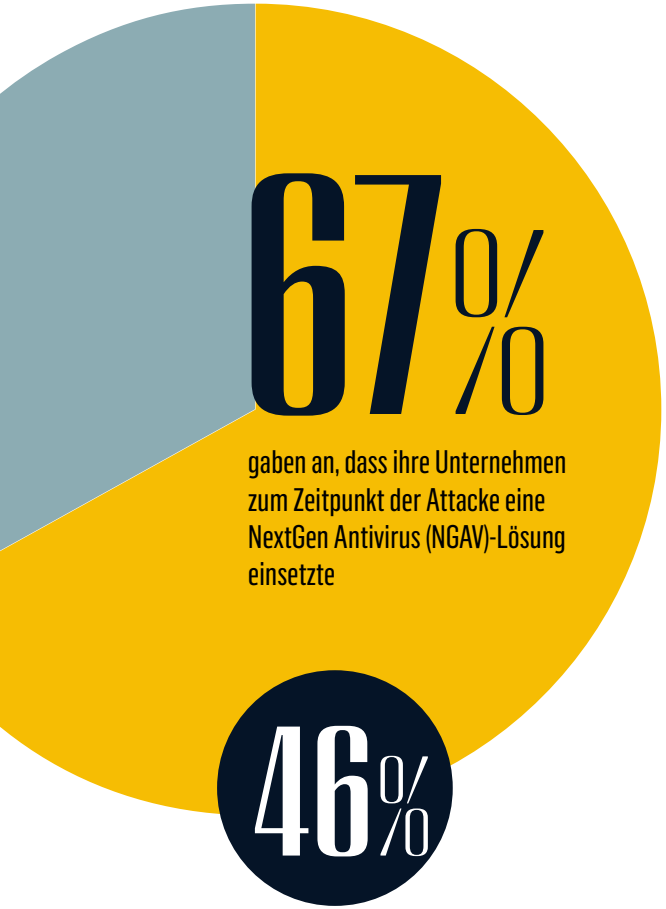
49%

gaben an, dass der Angriff erfolgreich war, weil sie keine wirksamen Security-Lösungen vor Ort hatten

Alle diese Indikatoren weisen auf eine **signifikante Abkoppelung von wahrgenommener Bedrohung zu der tatsächlichen Gefahr für Unternehmen** hin. Diese Trennung wird mit dem Ergebnis demonstriert, dass **ein Fünftel (20 %) glaubte, dass ihr Unternehmen niemals Ziel einer Ransomware-Attacke sein würde**. Die Gründe für dieses trügerische Gefühl der Sicherheit mögen in der kleinen Unternehmensgröße oder Einbindung in einer spezialisierten Branche liegen, die Immunität suggerierten. Welche Gründe auch immer eine Rolle spielten: Die Erkenntnisse zeigen deutlich, dass einige Unternehmen kein klares Verständnis von dem potenziellen Risiko haben, das Ransomeware-Angriffe darstellen.

Eine weitere wahrnehmbare Abkoppelung zeigt sich in der Studie dadurch, dass **63 % aller Befragten angaben, dass sie glaubten, dass es sich bei den Angreifern um komplex agierende, staatliche Bedroher (Advanced Persistent Threat – Fortgeschrittene, anhaltende Bedrohung) handelte**. Dies, trotzdem die überwältigende Mehrheit der dokumentierten Ransomware-Angriffe von nicht-staatlichen, cyberkriminellen Organisationen ausgeführt wurde – mit Ausnahme des finanzschwachen Nord-Koreas in begrenztem Umfang. Mit dieser Annahme war die Transportbranche (64 %) im oberen Durchschnitt, der Einzelhandel (46 %) unterdurchschnittlich vertreten.

Darüber hinaus, obwohl **89 % aller Befragten angaben, dass sie als Kandidat für einen Ransomware-Angriff** am Wochenende/in der Urlaubszeit **infrage kamen**, sagte **knapp die Hälfte (49 %), dass die Attacke, die ihr Unternehmen bereits erlitt, erfolgreich war, weil sie über keine funktionierende Security-Lösung verfügten**. Dies ist ein weiterer Schlüsselfaktor für die Diskrepanz zwischen dem wahrgenommenen Risiko und der unternehmerischen Bereitschaft, sich damit zu befassen. Im Einzelhandel (69 %) und in der Transportbranche (68 %) lagen die diesbezüglichen Rückmeldungen signifikant höher – ein Fakt, der die besondere Sorge zur Urlaubszeit unterstreicht.



Darüber hinaus gaben **nur 67 % an, dass ihre Unternehmen zum Zeitpunkt der Attacke eine NextGen Antivirus (NGAV)-Lösung einsetzte**, also einen Lösungsansatz, der AI-/Automatisiertes-Lernen-Kapazitäten beinhaltet. Dieser hat sich als hoch effektiv erwiesen gegen die beiden bekannten und zuvor nie gesehenen Malware-Varianten, gegen die Ausnutzung von Sicherheitsschwachstellen und noch weiter entwickelte Angriffe, die neben anderen auch Druckmittel wie dateilose Attacken oder schädliche Makros einsetzen. Der Einzelhandel (57 %) liegt dabei knapp über dem Durchschnitt, während die Transportbranche (84 %) signifikant höher liegt.

NGAV-Lösungen waren bisher hoch effektiv gegen solche Vorgehensweisen, vor allem in Netzwerken, die air-gapped oder anderweitig isoliert bleiben müssen, auch weil diese Lösungen selten Updates benötigen, um effektiv zu bleiben. Dennoch haben sie einige Defizite in ihrer Abwehrkompetenz, wenn sie nicht Teil einer vielschichtigen Lösung außerhalb des alleinigen AI/ML-Modells sind.

Die Studie zeigte ebenfalls auf, dass **46 % aller Befragten sagten, dass ihre Unternehmen traditionelle, signaturbasierte Antivirus (AV)-Lösungen einsetzten,** als sie von einem Ransomware-Angriff getroffen wurden. Der traditionelle AV-Ansatz besteht seit mehreren Jahrzehnten und ist nach wie vor einigermaßen effektiv gegen die bisher bekannten Commodity-Malware-Stämme. Leider hängt seine Effektivität von einem langen Prozess ab, der menschliche Analysen und kontinuierliche Übergabe neuer Signaturen zur Erkennung bedingt, so dass traditionelle AV-Lösungen nicht effektiv gegen neue, polymorphische oder neu gepackte Malware-Stämme sein können. Sie liefern daher auch keinen Schutz gegen dateilose Angriffe, bösartige Makros oder andere fortschrifttliche Techniken.

Endpoint Detection & Response (EDR)-Lösungen sind konstruiert, um Attacken anzugehen, die Abwehrtools nicht beenden können, um besser proaktiv Bedrohungen aufzuspüren und diese im Nachgang forensisch zu untersuchen.

36%

sagten, dass ihr Unternehmen im Haus eine Detection and Response (EDR)-Lösung einsetzt

Weiterhin gaben **nur 36 % aller Befragten an, dass ihre Unternehmen eine Endpoint Detection and Response (EDR)-Lösung im Haus nutzten**, als sie angegriffen wurden. Der Einzelhandel (46 %) lag dabei über dem Durchschnitt, die Transportbranche (28 %) lag erheblich niedriger. Dies ist ein Resultat der wachsenden Forschung und kontinuierlichen Medienberichterstattung über die bisherigen, hochkarätigen Ransomware-Attacken, die klar aufzeigen, dass die Angreifer ihre Angriffssequenzen komplexer, also "niedriger und langsamer" gestalteten, um von den traditionellen und NextGen-AV-Lösungen unentdeckt zu bleiben. Die ausgeklügelteren RansomOps kommen meist nur durch Verhaltensauffälligkeiten zum Vorschein und/oder durch proaktives Aufspüren mittels Wirksamkeit einer EDR-Lösung.

Die Einführung von EDR-Tools erfolgte als Antwort auf die Schwächen beider – traditioneller und NextGen-AV-Lösungen, und mit ihr der entsprechende Paradigmenwechsel. Die Verteidiger realisierten, dass –wenn Angreifer fähig genug sind und über ausreichend Zeit und Ressourcen verfügten – sie letztendlich erfolgreich darin sein würden, in jedes Ziel einzudringen. EDR-Lösungen sind so konstruiert, dass sie Angriffe angehen, die herkömmliche Abwehrtools nicht beenden können, ebenso wie sie besser Bedrohungen aufspüren und im Nachgang forensisch untersuchen können.

EDR-Lösungen haben sich als so effektiv erwiesen, dass eine Ausführungsverordnung des Präsidenten kürzlich alle Bundesbehörden dazu aufforderte, "eine Endpoint Detection and Response (EDR)-Initiative einzusetzen, um die proaktive Erkennung von Cybersecurity-Vorfällen zu unterstützen", ebenso wie das "aktive Cyber-Aufspüren, -Eindämmen und -Aufbereiten sowie die Reaktionskompetenz bei Vorfällen."

ABSOLUTES RISIKO:

Der menschliche Faktor

Während wir bisher Prozesse und Technologien behandelt haben, umfasst der dritte und wohl wichtigste Aspekt jedes Sicherheitsnetzwerks die Menschen. Obwohl Mitarbeiter aller Unternehmensbereiche einbezogen sind, liegt unser Fokus hier ausschließlich auf den Verteidigern. Es ist längst schon kein Geheimnis mehr, dass der Sicherheitsbereich unter extremem Fachkräftemangel leidet, und dieser Mangel ist einer der wichtigsten Faktoren, der zu Stress und Burnout der Security Experten führt. Die Cybersecurity Workforce Studie 2020 (ISC)[2] schätzt, dass es 3,1 Millionen Security Stabsstellen gibt, die besetzt werden müssen, allein in den USA sind 879.000 Stellen offen.

Innerhalb dieser Cybereason Studie **verpassten in Reaktion auf eine Ransomware-Attacke 86 % aller Befragten ihren Urlaub oder ihr Wochenende mit Familie und Freunden**. Von diesen Befragten waren Verteidiger aus der Finanzbranche mit etwas unter Durchschnitt liegenden 71 % die auffälligsten Ausreißer, die angaben, dass sie ihren Urlaub oder ihr Wochenende wegen eines Angriffs unterbrechen mussten. Das mag daraus resultieren, dass Unternehmen der Finanzbranche im allgemeinen wegen gesetzlicher Vorgaben die ausgereiftesten Security-Programme haben und über mehr Ressourcen verfügen, um eine bessere Abwehr aufzustellen.

Eine der größeren Überraschungen der Studie war, **dass 70 % zugaben, während ihrer Reaktion auf einen Ransomware-Angriff am Wochenende oder während des Urlaubs alkoholisiert gewesen zu sein**. Dies stellt einen Risikofaktor für Unternehmen dar, der bezogen auf Vorfallsreaktionen und in Business-Kontinuitätsplänen nicht berücksichtigt wird. Der Einzelhandel (73 %) lag dabei etwas höher als der Durchschnitt, während die Transportbranche (80 %) signifikant höher lag. Die Branchen Maschinenbau (91 %) und Recht (81 %) hatten ebenfalls die höchsten Fallzahlen in der Personalberichterstattung zu Trunkenheit, während Medien (60 %), die Finanzbranche (63 %) und Produktion (67 %) die geringsten Werte aufwiesen. Personal mit der kürzesten Betriebszugehörigkeit war bei der Abwehr einer Attacke weniger wahrscheinlich angetrunken, während dies bei langjährigem Personal wahrscheinlicher war.

Regional betrachtet waren Spanien und Singapur mit 47 % und 54 %, die zugaben, während eines Ransomware-Vorfalls angetrunken gewesen zu sein, jeweils die positiven Außenseiter. Darüber hinaus war es in Unternehmen höherer Umsatzklassen wahrscheinlicher, dass das Personal zugab, während einer Vorfallsreaktion angetrunken gewesen zu sein.

VOM RISIKO ABGEKOPPELT:

Auswirkungen auf das Unternehmen

Die mangelnde Vorbereitung auf Ransomware-Attacken hat signifikante Auswirkungen auf betroffene Unternehmen. **60 % aller Befragten, sagten, dass Wochenend- und Urlaubs-Angriffe längere Zeit in Anspruch nahmen, um das Ausmaß der Situation einschätzen zu können**. Darüber hinaus sagten **50 %, dass es dann auch länger dauerte, um eine effektive Reaktion aufzusetzen**, und **33 % sagten, dass es eine signifikant längere Zeit brauchte, um sich vollständig von einem solchen Angriff zu erholen**.

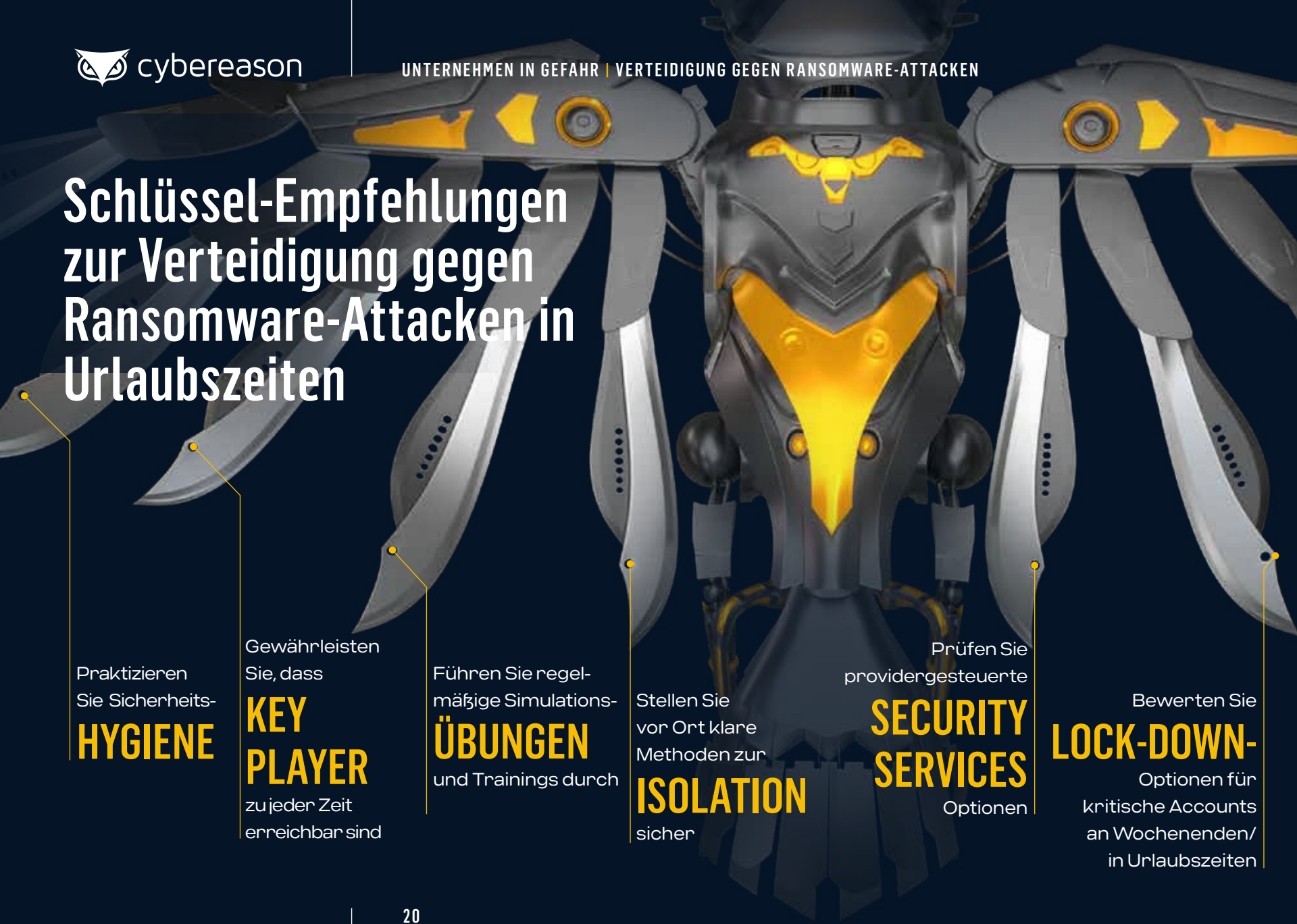
Ein Schlüsselfaktor in der Inkompetenz zum Aufsetzen einer rechtzeitigen Reaktion wurde durch **35 % der Befragten offenbart, die sagten, dass ein am Wochenende oder im Urlaub erfolgter Ransomware-Angriff es schwieriger machte, das richtige Team für eine Abwehrreaktion zusammenzustellen**. Diese Verzögerungen bei der Angriffsreaktion decken sich mit den Aussagen von **12 % aller Studienteilnehmer, die sagten, dass ihre Unternehmen bei solchen Angriffen im Ergebnis mehr Umsatz verloren,** wobei IT/Telekommunikation, Recht und die Transportbranche am signifikantesten davon betroffen waren.

Die **Auswirkungen auf das Unternehmen** durch eine Ransomware-Attacke beinhalten **Umsatzverluste, Schaden an der Unternehmensmarke, ungeplante Personaleinbußen und Störungen der Geschäftsabläufe**

Verteidigung gegen Ransomware-Attacken

Für Angreifer braucht es keine herausragenden kombinatorischen Fähigkeiten, um zu verstehen, dass die meisten Unternehmen wahrscheinlich an Wochenenden und während Urlaubszeiten am ungeschütztesten sind. Daher ist es eine solide Annahme, dass Bedroher ihre Attacken auf hoch bewertete Unternehmen in diesen Zeiten fortsetzen werden. Wie planen Unternehmen also, dieser Bedrohung entgegenzutreten?

Schlüssel-Empfehlungen zur Verteidigung gegen Ransomware-Attacken in Urlaubszeiten



Praktizieren Sie Sicherheits-
HYGIENE

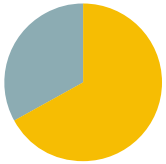
Gewährleisten Sie, dass
KEY PLAYER
zu jeder Zeit erreichbar sind

Führen Sie regelmäßige Simulations-
ÜBUNGEN
und Trainings durch

Stellen Sie vor Ort klare Methoden zur
ISOLATION
sicher

Prüfen Sie providergesteuerte
SECURITY SERVICES
Optionen

Bewerten Sie
LOCK-DOWN-
Optionen für kritische Accounts an Wochenenden/ in Urlaubszeiten



68%

gaben an, dass ihre Unternehmen planen oder bereits dabei sind, neue Technologien zu implementieren, um dem Risiko entgegenzuwirken

Um besser auf Ransomware-Angriffe vorbereitet zu sein, gab **eine Mehrheit der Befragten (68 %) an, dass ihre Unternehmen neue Technologien anschaffen**, um dem Risiko entgegenzuwirken. **Nur über die Hälfte (51 %) sagten, dass sie dabei sind, einen konkreten Notfallplan oder Richtlinien zu implementieren oder sie dies angehen**, wobei der Einzelhandel (45 %) ein wenig unter Durchschnitt und die Transportbranche (60 %) gut darüber liegt. **Fast die Hälfte (41 %) sagten, dass sie mehr Personal für diese Zeiten bereitstellen** – aber es kann noch mehr getan werden, um das Risiko von Ransomware-Angriffen an Wochenenden und in Urlaubszeiten zu reduzieren:

Praktizieren Sie gute Security-Hygiene durch Umsetzung eines Sicherheitbewusstseins-Programms für das Personal und stellen Sie sicher, dass für alle laufenden Systeme und andere Software regelmäßige Updates und Patches erfolgen, wobei die branchenbesten Sicherheitslösungen im Netzwerk eingesetzt werden sollten.

Stellen Sie sicher, dass das entscheidende Security Personal zu jeder Tageszeit erreichbar ist, da wichtige Abwehrmaßnahmen an Wochenenden/in Urlaubszeiten sonst verzögert erfolgen können. Es kann auch passieren, dass die richtigen Leute ihre E-Mails durch wegen der Attacke systembedingte Probleme nicht erhalten, oder sie nicht ans Telefon gehen, weil keine Erwartung formuliert wurde, dass sie im Notfall die Kommunikation im Auge halten sollen. Ein fest definierter Bereitschaftsdienst für Sicherheitsnotfälle außerhalb der Geschäftszeiten ist dann maßgeblich.

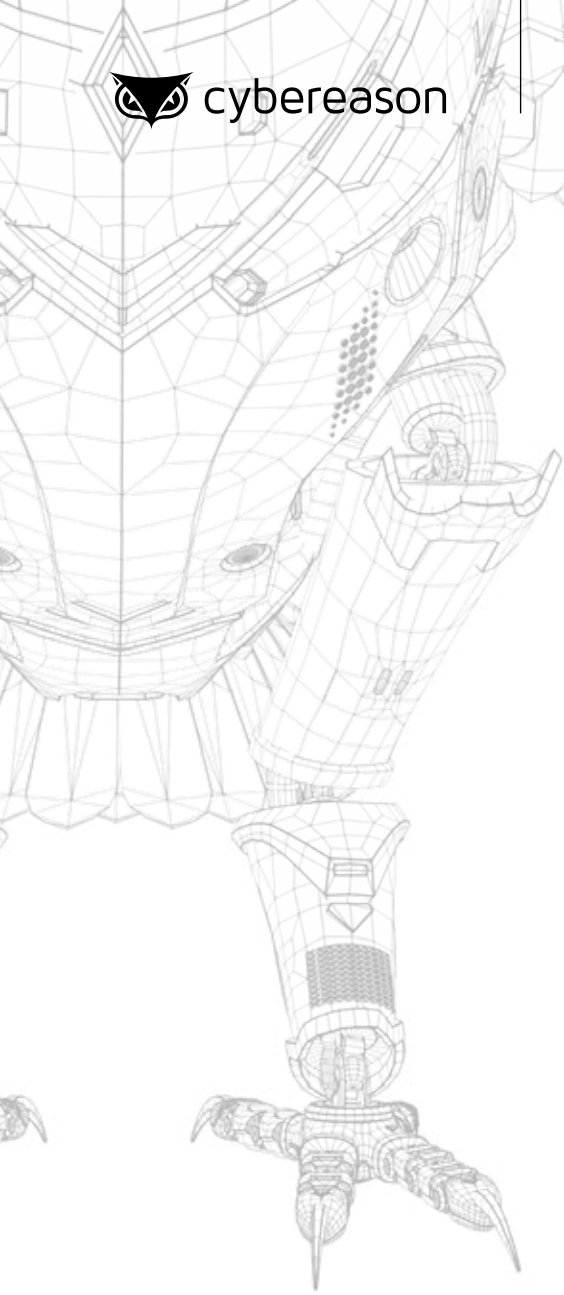
Führen Sie regelmäßige Simulationsübungen und -Trainings durch, die auch das Personal außerhalb des Security Teams integriert, wie die Rechtsabteilung, das Personalwesen, den IT-Support und alle anderen Abteilungen bis hin zur Vorstandsetage, um eine reibungslose Reaktion bei Vorfällen zu gewährleisten.

Teams
sollten qualifiziert sein,
einen Host abzukoppeln,
einen kompromittierten
Account
abzuschalten
und eine bösartige Domain
zu blockieren.

Stellen Sie sicher, dass vor Ort klar definierte Methoden zur Isolation verfügbar sind, die ein weiteres Eindringen der Ransomware in das Netzwerk stoppen und die Ausbreitung auf weitere Geräte verhindern. Teams sollten dafür qualifiziert sein, einen Host abzukoppeln, einen kompromittierten Account abzuschalten, eine bösartige Domain zu blockieren etc. Das Testen dieser Prozesse mit geplanten oder außerplanmäßigen Trainings mindestens in jedem Quartal ist notwendig, um sicherzugehen, dass das Personal und die Prozesse erwartungsgemäß funktionieren.

Prüfen Sie gesteuerte Security Services als Provideroption, falls Ihr Unternehmen personelle oder fachliche Defizite aufzeigt. Etablieren Sie vorher vereinbarte Reaktionsprozesse mit den Providern, damit diese im Notfall sofort nach dem vereinbarten Plan agieren können.

Prüfen Sie die Blockierung kritischer Accounts für Wochenenden/Urlaubszeiten, falls dies möglich ist. Der übliche Weg, den Angreifer zur Verbreitung der Ransomware über ein Netzwerk nehmen, ist die Erweitung der Admin-Rechte auf der Domain, um dann die Ransomware anzuwenden. Diese Accounts mit höchsten Rechten werden in vielen Fällen an Wochenenden oder Urlaubszeiten selten gebraucht. Teams sollten hochsichere, nur im Notfall einzusetzende Accounts im aktiven Verzeichnis anlegen, die nur genutzt werden, wenn andere operative Accounts als Vorsichtsmaßnahme deaktiviert sind oder der Zugriff darauf während einer Ransomware-Attacke nicht mehr möglich ist.



Die Strategie vertraut auf die Annahme, dass die Wahrscheinlichkeit, dass die Zugangsdaten zu diesen Accounts kompromittiert werden, denkbar gering sein sollte. Die Accounts werden fast nie genutzt, so dass sie potenziellen Bedrohungen kaum ausgesetzt sind. Das Security Operation Center kann diese Accounts nutzen, um alle anderen Domain-Admin-Accounts am Wochenende/in Urlaubszeiten zu deaktivieren und diese für die regulären Betriebszeiten oder – falls notwendig – im Notfall wieder zu reaktivieren. Es mag als ein umständlicher Prozess erscheinen, aber dies ist nichts im Vergleich zu den Prozessen, die nach einem erfolgreichem Ransomware-Angriff zur Entschlüsselung und Wiederherstellung von Hunderten oder Tausenden verschlüsselter Endpoints gefahren werden müssen. Es gibt weitere Optionen, um ähnliche Sicherheitsvorkehrungen mit einem VPN-Zugang zu schaffen, dessen Verfügbarkeit an Wochenenden auf die betrieblichen Anforderungen limitiert ist.

Genießen Sie in Ruhe Ihren Urlaub

Cyber-Attacken und Ransomware kommen in allen Formen und Größen daher. Manche Angriffe sind simpel, manche ausgeklügelt und komplex. Manche Bedroher sind durchschnittliche Cyberkriminelle, manche sind staatliche Gegner mit erheblichen Ressourcen. In der Realität ist dies alles unwichtig. Verteidiger müssen alle Attacken abwehren – unabhängig der Art des Angreifers oder der Rafinesse des Angriffs.

Sie brauchen mehrschichtige Plattformen, die **Verhaltens-Indikatoren** (IOBs) nutzen, um die Ransomware-Attacke zu identifizieren und die Angriffskette zu beenden

Wenn Ihre Daten einmal verschlüsselt sind, gibt es keine weiteren Optionen. Der einzig effektive Weg zur Bekämpfung von Ransomware ist, sie direkt zu Beginn noch vor der Infiltration abzuwehren. Viele Tools vertrauen auf "Indicators of Compromise" (IOCs) – wobei der Name bereits impliziert, dass die auffälligen Daten nicht entdeckt werden, bevor eine Kompromittierung erfolgt ist. Sie benötigen eine mehrschichtige Plattform, die Verhaltsindikatoren ("Indicators of Behaviour/IOBs) nutzt, um Ransomware-Attacken zu identifizieren und ihre Angriffskette zu beenden, unabhängig dessen, ob sie jemals zuvor entdeckt wurde – und bevor der Schaden eingetreten ist.

Dies beginnt damit, die richtigen Tools einzusetzen. Cybereason ist ungeschlagen im Kampf gegen Ransomware. Die Fähigkeit, IOBs zu verstehen, kombiniert mit einem betriebszentrierten Ansatz, der eine vollständige Sichtbarkeit über alle schädlichen Aktivitäten bietet – kurz: MalOp™ – ermöglicht Cybereason, Ransomware-Attacken früher zu erkennen, viel schneller darauf zu reagieren und sie sofort auszuschalten.

Sie brauchen Auszeiten. Sie verdienen es, auf der Geburtstagsfeier ihres Kindes zu sein, Zeit mit ihrer Familie zu verbingen und ihre Urlaubszeit zu genießen. Cybereason widmet sich ganz der Kooperation mit Verteidigern, um Cyber-Attacken von Endpoints zu den Unternehmen und überall hin zu beenden – moderne Ransomware eingeschlossen. Wir helfen Ihnen dabei, dass Sie Ihre Wochenenden und Urlaubszeiten in Ruhe genießen können – ganz sicher!

STUDIENMETHODIK

Die Studie wurde im September 2021 von Censuswide durchgeführt und bezog Cybersecurity-Experten aus der ganzen Welt ein. Ihnen wurden Schlüsselfragen zu ihren Erfahrungen mit und Vorbereitungen gegen Ransomware-Attacken in Urlaubszeiten und Wochenenden gestellt. Censuswide befragte 1.206 Cybersecurity Experten in Unternehmen mit mehr als 700 Mitarbeitern aus den USA, Großbritannien, Frankreich, Deutschland, Italien, Singapur, Spanien, Südafrika und den Vereinigten Arabischen Emiraten. Alle Studienteilnehmer waren binnen der letzten 12 Monate Opfer eines Ransomware-Angriffs während Urlaubs- oder Wochenendzeiten. Daher eigneten sie sich perfekt für Einblicke zu den erlebten Auswirkungen des Angriffs und Aussagen dazu, was sie planen, um zukünftig anders zu agieren.

ÜBER CYBEREASON

Cybereason ist der Branchenführer in modernster Cyber-Sicherheit. Unsere innovativen Abwehrmechanismen bieten zukunftsorientierten Schutz vor Angriffen für alle Endpunkte Ihres Unternehmens und darüber hinaus – überall dort, wo Bedrohungen stattfinden können. Die Cybereason Defense Platform kombiniert die branchenweit besten Erkennungs- und Abwehrmaßnahmen (EDR und XDR), Virenschutz der nächsten Generation (NGAV) und proaktive Bedrohungssuche, um eine kontextbezogene Analyse der Malops (malicious operation) zu ermöglichen. So können Verteidiger Cyberangriffe von Endgeräten aus und von überall beenden. Cybereason ist ein privates, internationales Unternehmen mit Hauptsitz in Boston, London und München sowie Kunden in mehr als 45 Ländern.
Erfahren Sie mehr unter: **www.cybereason.com/de**