WHITEPAPER

Malwarebytes

DER WEG ZUR CYBER-WIDERSTANDSFÄHIGKEIT:

Leitfaden für Unternehmen im Zeitalter der digitalen Transformation

Juni 2019

Einleitung

Die digitale Transformation hat die Geschäftstätigkeit von Unternehmen revolutioniert. Die Art und Weise, wie sie Marktanforderungen erfüllen und die Zufriedenheit ihrer Kunden gewährleisten, hat sich grundlegend verändert. Gleichzeitig sind die Datenmengen und die Anzahl der Endpunkte mit der Verbreitung von mobilen und IoT-Geräten explosionsartig angestiegen. Beides erfordert einen sorgfältigen Schutz gegen Cyberangriffe.

Eine zuverlässige Cybersicherheit ist seit jeher eine wesentliche Komponente bei der Umsetzung der digitalen Transformation in einem Unternehmen. Traditionelle Vorgehensweisen zum Schutz der Daten mit festen Firewalls und signaturbasierten Antiviruslösungen reichen in einer Welt polymorpher Angriffe und mobiler Mitarbeiter einfach nicht mehr aus. Die andauernde Erweiterung der Angriffsziele gestaltet den Schutz schwieriger und macht einen erfolgreichen Angriff immer unvermeidbarer. Laut einer Studie von Malwarebytes aus dem Jahr 2019 zur Cyber-Widerstandsfähigkeit, bei der mehr als 350 Sicherheitsexperten befragt wurden, gehen 75 Prozent aller Organisationen davon aus, dass sie in den nächsten ein bis drei Jahren vermutlich Opfer einer Sicherheitsverletzung werden.

Infolgedessen stellen die Organisationen ihre Investitionen für den Aufbau einer Cyber-Widerstandsfähigkeit auf den Prüfstand. Zu diesem Zweck müssen Organisationen ihre Mitarbeiter, Prozesse und Technologien bewerten, um zu gewährleisten, dass sie den bestmöglichen Schutz haben, den Geschäftsbetrieb auch während eines Cyberangriffs aufrechterhalten können und sich schnell von einem Angriff erholen können. Eine fehlende Cyber-Widerstandsfähigkeit kann astronomische Kosten verursachen – von der Einstellung des Geschäftsbetriebs bei kleineren Unternehmen bis hin zu Betriebsunterbrechungen mit verheerenden Auswirkungen bei größeren Unternehmen. Eine einzelne Sicherheitsverletzung kann zu Verlusten von bis zu 4,2 Millionen USD führen, und zwar in Form von Kundenfluktuation, verstärkten Aktivitäten zur Kundenakquise, Imageschäden und vermindertem Goodwill.[1]

Um diesem Ziel mehr Gewicht zu verleihen, bitten Führungskräfte und Vorstandsmitglieder die CISOs zunehmend darum, ihre Strategie für eine Cyber-Widerstandsfähigkeit zu präsentieren und die Verantwortung für die nahtlose Umsetzung des Plans zu übernehmen. Die Malwarebytes-Studie zur Cyber-Widerstandsfähigkeit hat ergeben, dass mehr als 87 Prozent aller Sicherheitsexperten die Sicherheits-Response-Pläne mindestens einmal pro Jahr mit ihren Vorgesetzten und dem Vorstand besprechen müssen. Die CISOs müssen daher bereit sein nachzuweisen, dass sie eine Strategie für die Cyber-Widerstandsfähigkeit haben – die nicht nur Daten, Endpunkte und Betriebsbereitschaft des Unternehmens schützt, sondern auch anhaltendes Geschäftswachstum sicherstellt.

Anschließend untersucht diese Studie die aktuellen Markteinflüsse, die sich darauf auswirken, wie eine Organisation Cyber-Widerstandsfähigkeit erreichen will, die wichtigsten Methoden, die zur Erzielung der Cyber-Widerstandsfähigkeit angewendet werden sollten, sowie die Gründe, wieso die Cyber-Widerstandsfähigkeit eine Organisation zu einem digital geprägten Unternehmen machen kann, das sich stark auf Wachstum konzentriert.

Trends mit Gefährdungspotenzial für Endpunkte

Die Art und Weise, in der Unternehmen Geschäfte tätigen, hat sich in den letzten Jahren zweifellos deutlich verändert. Geschäftsförderliche Technologien und Systeme, wie Kollaborationswerkzeuge, BYOD und Cloudservices, erleben Innovationen in atemberaubender Geschwindigkeit. Infolgedessen musste die IT ihren strategischen Schwerpunkt immer wieder neu ausrichten, um sich den Entwicklungen anzupassen. Und inmitten all dieser Umbrüche erleben die Unternehmen eine Annäherung zentraler Markttrends, die den Endpunkt zum neuen Perimeter und damit die Priorisierung der Cyber-Widerstandsfähigkeit zur neuen unternehmerischen Notwendigkeit gemacht haben.

Erweiterung der Angriffsziele

Ein entscheidender Trend, der die Bedeutung der Cyber-Widerstandsfähigkeit unterstreicht, ist die Vergrößerung der unternehmerischen Angriffsflächen infolge der Cloudnutzung und der Gerätemobilität. Mit der Einführung des Cloud Computing haben Unternehmen schnell den Wert und die Gelegenheit erkannt, Investitionen in Infrastruktur abzugeben und Ressourcen einzusparen. IDC prognostiziert, dass 67 Prozent der Investitionen in den Bereichen Unternehmensinfrastruktur und -software bis zum Jahr 2020 in cloudbasierte Angebote gehen werden.

Die Nutzung der Cloud und mit Mobilgeräten ausgestattete Mitarbeiter haben jedoch zur Verbreitung von verteilten Netzwerken geführt, die schwieriger zu schützen sind. Folglich haben Internetkriminelle mehr Möglichkeiten, Unternehmen anzugreifen. Durch die Vergrößerung der Angriffsflächen von Unternehmen stehen Unternehmen nun unter enormem Druck, um für Cyber-Widerstandsfähigkeit zu sorgen.

Steigender Wert von Daten

Das Voranschreiten der digitalen Transformation und künstlichen Intelligenz sowie die Verwendung von Big Data hat zum Anstieg von auf Erkenntnissen basierten Geschäften geführt – wobei Daten Wachstum durch Marktstörungen ermöglichen, Produktivität erhöht wird und neue Einnahmequellen eröffnet werden. Unternehmen haben sich branchenübergreifend dahingehend entwickelt, dass die Daten, die sie besitzen, ihr Flaggschiffprodukt sind. So berichten 63 Prozent erfahrener Entscheidungsträger, dass Big Data jetzt ein Einnahmentreiber sind und für die Unternehmen genauso wertvoll werden wie ihre bestehenden Produkte und Dienstleistungen.[2]

Den Wert von Unternehmensdaten erkennen auch Internetkriminelle zunehmend. Mit gestohlenen personenbezogenen Daten können sie auf dem Schwarzmarkt 1000 USD pro Datensatz verdienen[3] sowie Social-Engineering-Betrügereien und eine Vielzahl anderer Straftaten begehen. Der Zugang zu diesen begehrten Daten ist die treibende Kraft hinter den Cyberangriffen auf Unternehmensnetzwerke, die unerbittlich Mitarbeiterendpunkte verfolgen, um einen Fuß in die digitale Tür des Unternehmens zu bekommen.[4] 70 Prozent der Unternehmen berichten, dass ihre Daten für ihren Geschäftsbetrieb sehr wichtig bis unternehmenskritisch sind.[5] Damit ist Cyber-Widerstandsfähigkeit unverzichtbar für Organisationen, um zu gewährleisten, dass ihre Daten zuverlässig geschützt und jederzeit zugänglich sind.

Immer ausgeklügeltere Angriffe

Seit den Anfängen der Cyberangriffe haben die Bedrohungsakteure ihre Taktiken immer mehr verfeinert, um einer Aufdeckung zu entgehen und Zugang zu Unternehmensendpunkten zu erhalten. Ursprünglich wurden Endpunkte nur als Einstieg in das Unternehmensnetzwerk zu wertvolleren Zielen angegriffen. In den letzten Jahren haben automatisierte Angriffe, wie Ransomware und sich lateral verbreitende Exploits, wie SMB-Schwachstellen, die Opferzielgruppen jedoch „demokratisiert“, d. h. der Endpunkt selbst und die darauf befindlichen Daten sind das Hauptziel.

Und Unternehmen jeder Größenordnung sind davon betroffen. Internetkriminelle haben Darknet-Marktplätze geschaffen, die für Ihre Gleichgesinnten ein Ökosystem für die Zusammenarbeit und die Entwicklung ausgeklügelter Angriffspakete zu minimalen Kosten bieten. Dies wiederum hat es den Bedrohungsakteuren ermöglicht, mehr Ziele ins Visier zu nehmen und Unternehmen jeder Größenordnung anzugreifen. Und schon ein einziger erfolgreicher Angriff kann den Geschäftsbetrieb beeinträchtigen und Responseteams wochenlang beschäftigen, bis das Netzwerk erfolgreich wiederhergestellt wurde.

Komplexe Konformitätsanforderungen mit zunehmender Strafkomponente

Vorschriften sind ein notwendiger Bestandteil des digitalen Zeitalters, um gesetzliche Vorgaben zu schaffen, die sicherstellen, dass die Unternehmen angemessene Maßnahmen zum Schutz der sensiblen Daten ihrer Kunden ergreifen. Mittlerweile haben mehr als 100 Länder weltweit umfassende Datenschutzgesetze erlassen.

Zwischen den weit greifenden internationalen Vorschriften, wie der Global Data Privacy Regulation (GDPR), branchenspezifischen Compliance-Regelwerken und der Gesetzgebung auf Bundeslandebene müssen die meisten Organisationen branchenübergreifend ein bestimmtes Vorschriftenwerk erfüllen. Und häufig sind Unternehmen von mehreren, widersprüchlichen Vorschriften betroffen.

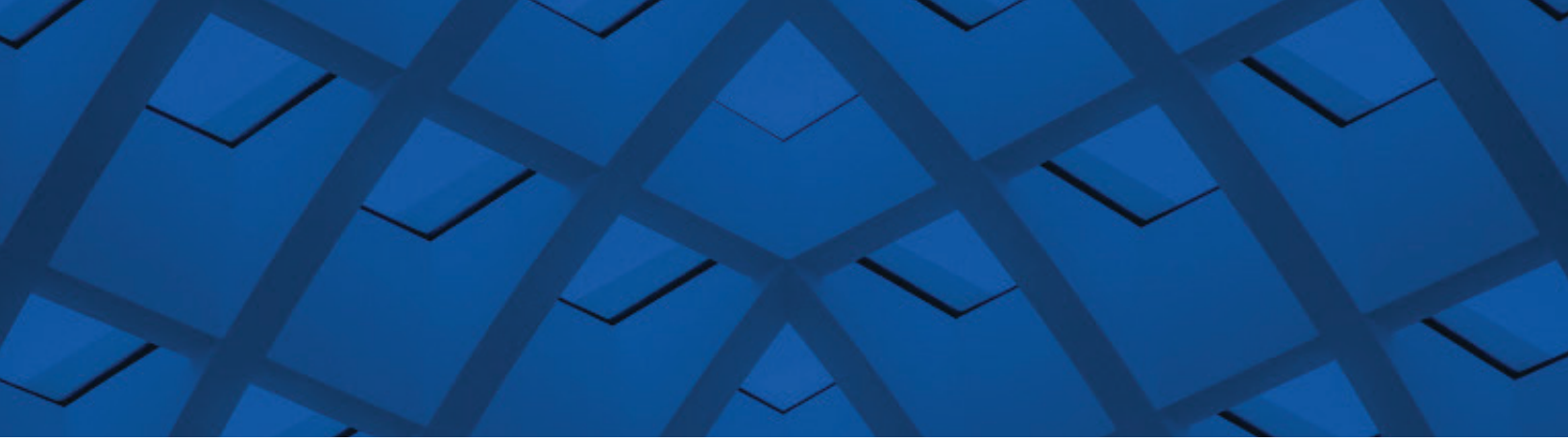
Das sich ständig ändernde regulatorische Umfeld hat ein zunehmend komplexes Compliance-Labyrinth geschaffen, durch das die Organisationen navigieren müssen. Die Nichterfüllung von Vorschriften kann hohe Strafen nach sich ziehen und zu Unternehmensgebilden führen, die bei einem Vorfall nicht mit der nötigen Flexibilität und Präzision reagieren können.

Steigende Kosten von Sicherheitsverletzungen und Abwehrmaßnahmen

Erfolgreiche Sicherheitsverletzungen sind für Organisationen sehr kostspielig, was Umsatzeinbußen, Kundenfluktuation und Datenverlust betrifft. Außerdem erholen sich Unternehmen nur schwer von Betriebsunterbrechungen und einem beschädigten Markenwert. Denken Sie nur an die im Juli 2015 veröffentlichten 32-GB-Hacker, die personenbezogenen Daten der gesamten Kundendatenbank von Ashley Madison offenlegten, nachdem sich das Unternehmen geweigert hatte, ein gefordertes Bitcoin-Lösegeld zu bezahlen. Später waren die Benutzer, deren Daten veröffentlicht worden waren, mit einer Sammelklage in Höhe von 11,2 Millionen USD gegen das Unternehmen erfolgreich.[6]

Die Kosten von Sicherheitsverletzungen und für Abwehrmaßnahmen steigen stetig. Laut dem Ponemon Institute betrifft die durchschnittliche Sicherheitsverletzung sage und schreibe 24.615 Datensätze weltweit und kostet 3,8 Millionen USD.[7] Wenn die Kosten einer Sicherheitsverletzung ein Unternehmen nicht in den Ruin treiben, kann es allerdings oft Jahre dauern, bis sich die Organisation wieder erholt und ihre frühere Finanzkraft wieder erlangt hat.

Diese zusammenspielenden Trends haben den Unternehmensendpunkt als neue vorderste Verteidigungslinie gegen Sicherheitsverletzungen in Stellung gebracht. Außerdem zeigen sie auf, wie dringend und wichtig es ist, dass eine Organisation in der Lage ist, angesichts des unausweichlichen Angriffs für eine wirkungsvolle Cyber-Widerstandsfähigkeit zu sorgen.



Herausforderungen auf dem Weg zur Cyber-Widerstandsfähigkeit

Für CISOs liegt die Verantwortung für den Aufbau einer unternehmensweiten Cyber-Widerstandsfähigkeit bei der Geschäftsführung. Die Umsetzung der Cyber-Widerstandsfähigkeit hat jedoch einige Probleme bereitet. Ein Drittel von Sicherheitsexperten haben keinen Response-Notfallplan für Sicherheitsverletzungen. Wenn diese Organisationen also angegriffen werden, werden sie sich nur langsam wieder davon erholen. Und das in einem Umfeld, in dem mehr als drei Viertel aller Organisationen glauben, dass sie in den nächsten drei Jahren Opfer einer Sicherheitsverletzung werden.[8]

Dies ist eine hoch riskante Lücke zwischen der Planung einer Cyber-Widerstandsfähigkeit und der Bereitschaft eines CISO, den Plan umsetzen zu können. Die großen Schwierigkeiten, einer Organisation eine zuverlässige Cyber-Widerstandsfähigkeit bereitzustellen, verlagern sich über die Cybersicherheitspfeiler Menschen, Prozesse und Technologie einer Organisation.

Mangel an qualifiziertem Personal angesichts zunehmender Komplexität

Die Verfügbarkeit von ausgebildetem Personal mit ausgewiesener Sicherheitskompetenz stellt nach wie vor eine Herausforderung dar. Schließlich berichten 56 Prozent aller Organisationen, dass sie kein ausgebildetes Personal einstellen und halten können.[9] Leider ist dies ein systemisches Problem, dessen Ende noch nicht absehbar ist. Laut Cybersecurity Ventures wird es bis zum Jahr 2021 3,5 Millionen unbesetzte Stellen im Bereich Cybersicherheit geben.

Die Bedrohungen entwickeln sich immer weiter. Da stellt der allgegenwärtige Mangel an Ressourcen und Kompetenzen im Bereich Cybersicherheit eine tagtägliche Herausforderung für CISOs dar. Denn sie müssen ihre Mitarbeiter regelmäßig weiterbilden und die betrieblichen Schwierigkeiten bewältigen, die mit der Rekrutierung von Kandidaten für offene Stellen einhergehen.

Fehlender Bestand an wichtigen Daten und Systemen

Cyber-Widerstandsfähigkeit erfordert eine Vorbereitung durch Identifizieren und Priorisieren der wichtigsten Daten, Endpunkte und Systeme des Unternehmens, die für die Aufrechterhaltung des Geschäftsbetriebs bei einem Vorfall von entscheidender Bedeutung sind. Dennoch geben 46 Prozent aller Sicherheitsexperten an, dass ihre Cyber-Widerstandsfähigkeit durch einen Mangel an Sichtbarkeit von Anwendungen und Datenassets beeinträchtigt wird.[10]

Die größte Hürde: Unternehmen können nicht inventarisieren, was sie nicht sehen können. Die CISOs sehen sich durch die Nutzung der Cloud und mobiler Geräte einer immer größeren Angriffsfläche gegenüber. Damit wird es immer schwieriger, alle Daten und die Schatten-IT der Organisation zu inventarisieren und ihre Speicherorte festzuhalten. Ohne dieses Verständnis können Unternehmen nicht sicherstellen, dass alle Systeme angemessen geschützt sind, oder ihre Incident-Response-Methoden mit der nötigen Strenge durchsetzen.

Technische Fortschritte und Herausforderungen

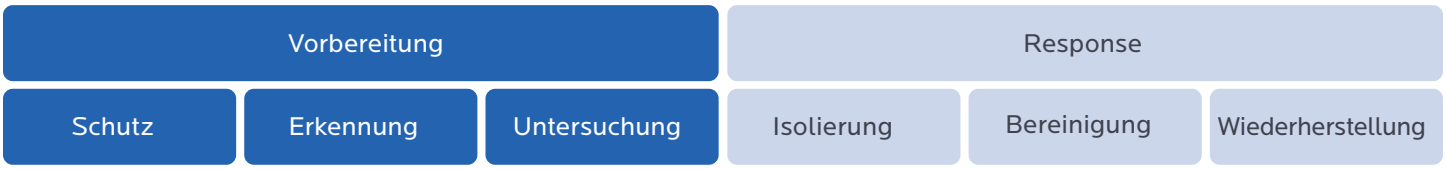
Die Fortschritte bei geschäftsförderlichen Technologien haben eine sich permanent ändernde digitale Umgebung geschaffen, die IT- und Sicherheitsteams verwalten und schützen müssen. Unternehmen nutzen Videokollaborationsplattformen, beteiligen sich an der Revolution der sozialen Medien, verwenden das Modell Anything-as-a-Service und statten ihre Mitarbeiter mit Smartphones aus, um nur einige der zahllosen IT-basierten Geschäftstrends zu nennen.

Parallel dazu haben sich die Sicherheitstechnologien geändert und wurden um neue Kontrollen erweitert, um die Sicherheitslücken, die von diesen Unternehmenstechnologien geschaffen wurden, zu schließen und innovativen Angreifermethoden entgegenzuwirken. Die Infrastruktur der heutigen Sicherheitsabteilung (SOC) besteht sogar aus mindestens 20 Sicherheitsanwendungen.[11] Zwischen Geschäfts- und Sicherheitswerkzeugen gibt eine Unzahl von Technologien, die die IT in einer sich ständig verändernden Umgebung beherrschen muss.

> **46 %**
>
> aller Sicherheitsexperten beklagen, dass ihre Cyber-Widerstandsfähigkeit durch einen **Mangel an Sichtbarkeit von Anwendungen und Datenassets** behindert wird.

Automatisierung ist der Schlüssel zur Cyber-Widerstandsfähigkeit

> Die Anwendung einer Methode zur Erlangung der Cyber-Widerstandsfähigkeit, die das Sicherheitsregelwerk von der Vorbereitung bis zur Response abdeckt, minimiert die Auswirkungen eines Cyberangriffs und stellt sicher, dass die CISOs die Systeme schnell wiederherstellen und die Geschäftskontinuität aufrechterhalten können. Die Organisationen sollten vor dem Hintergrund der Unternehmensherausforderungen, denen sie zur Erlangung der Cyber-Widerstandsfähigkeit gegenüberstehen, identifizieren, wo die Cyber-Widerstandsfähigkeit im Regelwerk Lücken aufweist, und Maßnahmen zur Automatisierung in diesen Bereichen ergreifen.



Automatisierungsmechanismen sind eine wirksame Methode zum Stärken der Cyber-Widerstandsfähigkeit, führen zu besseren Sicherheitsergebnissen und bieten bedeutende Vorteile. Unternehmen, die zu hundert Prozent auf Sicherheitsautomatisierung setzen, verzeichnen beim Umgang mit einer Datensicherheitsverletzung im Durchschnitt zunehmende Einsparungen in Höhe von 1,55 Millionen USD.[12]

Automatisierung bietet den CISOs eine Möglichkeit, ihre Investition zu maximieren und den Druck von anhaltenden Einschränkungen im Personal- und Ausbildungsbereich zu nehmen. Automatisierung ist skalierbar und muss nicht schlafen. Sie bedeutet auch einen proaktiven Umgang mit der Sicherheit, mit dem nach Bedrohungen gesucht werden kann, an die das Sicherheitsteam möglicherweise nicht denkt.

Automatisierte Erkennung durch künstliche Intelligenz und maschinelles Lernen

Ein gutes Sicherheitskonzept basiert auf aussagekräftigen Bedrohungsdaten. Durch die Automatisierung von Bedrohungsdaten mit modernen Analysetechniken, künstlicher Intelligenz und maschinellem Lernen haben Organisationen bessere Möglichkeiten der Bedrohungserkennung und können genauso schnell reagieren wie Internetkriminelle ihre Methoden entwickeln. Außerdem stellen diese Methoden die beste Herangehensweise zur Erkennung unbekannter Bedrohungen dar.

Durch die Automatisierung von Bedrohungsdaten mit moderner, skalierter Analytik werden Bedrohungen, die von früheren Verteidigungsmechanismen der Unternehmen unerkannt blieben, deutlich öfter erkannt. Bei richtigem Einsatz trägt sie auch zur Verringerung falscher Alarme und falscher positiver Ergebnisse von Erkennungssystemen bei.

Unternehmen wissen den Wert automatisierter Erkennung bereits zu schätzen. Laut der Malwarebytes-Studie zur Cyber-Widerstandsfähigkeit haben 59 Prozent aller Sicherheitsexperten die Bedrohungserkennung automatisiert und 45 Prozent planen, mehr in diese Richtung zu gehen.

Automatisierte Response ohne Beeinträchtigung der Geschäftstätigkeit

Ein erfolgreicher Cyberangriff geschieht schnell. Schadsoftware wird häufig schnell lateral vom ersten betroffenen Endpunkt zu anderen Endpunkten und Systemen in der Umgebung verbreitet. Unternehmen sehen sich ständig mit knappen Ressourcen und Kompetenzen konfrontiert, die lange Incident-Response-Zeiten verursachen. Unternehmen brauchen im Durchschnitt 197 Tage, bis sie einen Angriff identifizieren, und weitere 69 Tage, bis sie ihn eingedämmt haben.[13]

Durch die Investition in Werkzeuge, die Response-Mechanismen automatisieren, kann die Cyber-Widerstandsfähigkeit eines Unternehmens beträchtlich verbessert werden. Die Anforderungen an eine automatisierte Response sollten Funktionen umfasen, die es Organisationen ermöglichen, aktiv auf eine Bedrohung zu reagieren. Hierzu gehören die Fähigkeiten des automatischen Isolierens, Behebens und Wiederherstellens.

Das Eindämmen eines Angriffs ist der erste Response-Schritt. Incident-Response-Teams können die Beseitigung von Schadsoftware wirkungsvoller planen, wenn ein Angriff erfolgreich isoliert und sichergestellt wurde, dass er keinen weiteren Schaden mehr anrichten kann. Aus diesem Grund haben 47 Prozent aller Sicherheitsmanager die Isolierung infizierter Endpunkte automatisiert. Weitere 53 Prozent planen zeitnahe Investitionen in die automatisierte Endpunktisolierung.[14]

Die automatisierte Isolierung sollte Organisationen die Flexibilität bieten, eine Infektion einzudämmen, während die Auswirkung auf den Benutzer minimiert wird. Das bedeutet, dass eine Bedrohung am Endpunkt durch Isolierung auf Netzwerk-, Geräte- und Prozessebene eingedämmt wird. Diese Eindämmungsmethoden erschweren der Schadsoftware auch Rückmeldungen zu ihrem Ursprung, um eine Command-and-Control-Kommunikation anzustoßen, wodurch sie keinen weiteren Schaden anrichten kann. Unternehmen sollten auch die Wiederherstellung nach Ransomware-Angriffen in den Anforderungskatalog ihrer automatisierten Response aufnehmen. Diese Funktion sollte Just-in-time-Endpunktsicherungen umfassen, mit denen die Uhr automatisch zurückgedreht und die Auswirkung eines Ransomware-Angriffs zunichte gemacht wird.

Die zweite Anforderung an eine erfolgreiche Response ist die automatisierte Beseitigung von Schadsoftware. Dadurch wird die Cyber-Widerstandsfähigkeit eines Unternehmens gestärkt, indem Systeme schnell und wirksam wiederhergestellt werden, ohne Zeit oder Expertise von Mitarbeitern in Anspruch nehmen zu müssen. Außerdem können CISOs damit Endpunkte skaliert bereinigen und die mittlere Response-Zeit des Unternehmens drastisch reduzieren.

Der Markt bewegt sich hin zu einer weit greifenden automatisierten Beseitigung von Schadsoftware ohne Entfernung der Schadsoftware von den Endpunkten. Immerhin berichten 54 Prozent aller Sicherheitsexperten, dass sie diese Funktion in ihr neues Arsenal für Cyber-Widerstandsfähigkeit aufgenommen hätten. Weitere 52 Prozent planen künftige Investitionen in diesem Bereich.[15]

Technologien mit einer gründlichen und automatisierten Beseitigung von Schadsoftware stellen den vertrauenswürdigen Zustand der Endpunkte im Unternehmen wieder her, in dem sie sich vor der Infektion befanden. Für eine moderne Cyber-Widerstandsfähigkeit sollten die Beseitigungsfunktionen auch die Erkennung und Entfernung dynamischer und verwandter Artefakte enthalten. Dies ist von entscheidender Bedeutung, um zu verhindern, dass Schadsoftware das Netzwerk erneut infiziert.

Automatisierte Orchestrierung über IT-Silos hinweg

Wenn Unternehmen die Orchestrierung integrierter Aufgaben der Endpunktsicherheit zwischen ihren komplexen und verteilten Sicherheitsökosystemen und Services automatisieren, dann optimieren, beschleunigen und vereinfachen sie Sicherheitsprozesse und Operationen. Durch die Automatisierung einfacher Aufgaben und die Ermöglichung der Prozessautomatisierung zwischen Sicherheitskontrollen erlangen Unternehmen eine Cyber-Widerstandsfähigkeit, die bei schnelleren Aktionen, die schützen und unmittelbar auf Angriffe reagieren, flexibel ist. Außerdem kann die Organisation mit koordinierten Workflow-Aktionen begrenzte Ressourcen besser einsetzen und verwalten.

Die Integrationsmöglichkeiten über das gesamte IT-Sicherheitspaket hinweg sind zahlreich. Angesichts der Bedeutung von Unternehmensendpunkten für die Geschäftskontinuität und ihrer Position an vorderster Front der Angriffsfläche einer Organisation sollten Unternehmen die automatisierte Orchestrierung für die Endpunktsicherheit und Verwaltungsfunktionen priorisieren.

Orchestrierungswerkzeuge, die eine Endpunktsichtbarkeit sowie die Möglichkeiten zum Koordinieren, Informieren und Ausführen der Schutz- und Beseitigungsbemühungen bieten, werden das Sicherheitskonzept und die Cyber-Widerstandsfähigkeit eines Unternehmens deutlich verbessern. Darüber hinaus sollten Organisationen eine cloudbasierte Verwaltung von Endpunkten vornehmen, die eine Sichtbarkeit mit Beseitigungskarten bieten. Damit wird gewährleistet, dass CISOs Response-Bemühungen koordinieren und den Fortschritt verfolgen können, wenn ein erfolgreicher Vorfall geschieht.

Die Vorteile der Cyber-Widerstandsfähigkeit genießen

> Automatisierung bietet weitreichende Vorteile. Unternehmen, die in Automatisierungsfunktionen investieren, genießen ein hohes Maß an Cyber-Widerstandsfähigkeit. So geben beispielsweise 71 Prozent aller Sicherheitsexperten an, dass mit Hilfe von Automatisierung die Response-Zeit für Erkennung, Response und Beseitigung von Schadsoftware sinkt. Kürzere Response-Zeiten wiederum führen zu beträchtlichen Einsparungen: Unternehmen, die eine Sicherheitsverletzung in weniger als 30 Tagen eindämmen, sparen 1 Million USD im Vergleich zu Unternehmen, die länger als 30 Tage dafür brauchen.[17]

Darüber hinaus wird mit kürzeren Response-Zeiten verhindert, dass gefährliche Infektionen Tausende von Endpunkten außer Gefecht setzen. Dies ist von entscheidender Bedeutung in der heutigen Welt der NSA-betriebenen Exploits, wie EternalBlue und EternalRomance, die dazu dienen, Bedrohungen lateral wie Flächenbrände durch Netzwerke zu verbreiten.

Unternehmen mit einer starken Cyber-Widerstandsfähigkeit verstehen den großen Wert ihrer Daten und implementieren entsprechende Pläne und Technologien für eine wirksame Cyber-Widerstandsfähigkeit. Wenn CISOs dies tun, können sie den Vorstandsmitgliedern stolz berichten, dass die Organisation den besten Gefahrenabwehrplan mit ausgeklügelten Widerstandsmaßnahmen hat, die den Betrieb aufrechterhalten, das Umsatzwachstum sichern und die Kundendaten sowie den Ruf des Unternehmens im Falle eines Angriffs schützen.

Zu guter Letzt sorgt Automatisierung auch für eine wirksamere SOC, die es Analytikern erlaubt, sich auf die einkommenswirksamen Initiativen des Unternehmens zu konzentrieren, die mehr Planung und Fachwissen erfordern (z. B. Analystenfunktionen der Ebene drei und vier). Die Mehrheit von SOC-Teams (54 Prozent) behauptet, dass sie mit Hilfe von Automatisierung ihre Sicherheitsaktivitäten besser priorisieren können.[18]

Mit diesem Ansatz werden die Ressourcen von den zeitaufwändigen Re-Imaging-Arbeiten und „Feuerlösch“-Aufgaben infolge von Budgeteinschränkungen oder mangelndem Fachpersonal befreit. SOC trägt so vielmehr zum Umsatz- und damit Unternehmenswachstum bei.

Schlussfolgerung

> Die digitale Transformation hat es ermöglicht, dass Unternehmen Daten nutzen, die Operationen optimieren, Wachstum beschleunigen und Kundenbindung stärken. Gleichzeitig ist Cybersicherheit zu einer Notwendigkeit geworden, um die wertvollen Daten des Unternehmens und die Geschäftsoperationen zu schützen.

Seitdem üben sich CISOs in der Gratwanderung zwischen Gefahrenabwehr und Budget- sowie Ressourceneinschränkungen. Eine optimale Cybersicherheit erfordert – für Menschen, Prozesse und Technologien – ein Investitionsvolumen, das viele Unternehmen entweder nicht tätigen wollten oder für das sie keine dringende Notwendigkeit sahen, bis sich die nicht vorhandene Cyber-Widerstandsfähigkeit auf ihren Gewinn auswirkte.

Letztendlich brauchen Unternehmen Mechanismen zum Automatisieren ihrer Cyber-Widerstandsfähigkeit, damit sie mit derselben Geschwindigkeit und mit denselben Ressourcen agieren können wie Internetkriminelle selbst. Die Markttrends bringen die Unternehmensendpunkte immer mehr an die vorderste Netzwerkfront, sodass CISOs Maßnahmen für die Widerstandsfähigkeit der Endpunkte ergreifen sollten.

Schließlich stellt die Cyber-Widerstandsfähigkeit sicher, dass der Geschäftsbetrieb weiterläuft und SOC-Teams zum Unternehmenswachstum beitragen. Indem Operationen unter Kontrolle gehalten, wertvolle Daten geschützt werden und Endpunkte die automatisierten Werkzeuge zum Abwehren von Angriffen erhalten, stellt die Cyber-Widerstandsfähigkeit sicher, dass die Unternehmen weiterhin neue Kunden gewinnen, während zufriedene Kunden bleiben und der Marktwert steigt.

[1] Ponemon Institute. 2018 Cost of Data Breach Study. Juli 2018.
[2] Capgemini. Big & Fast Data: The Rise of the Insight-Driven Business.
[3] CSO Online. What information in businesses do cybercriminals value?. November 2018.
[4] Malwarebytes. Cybersecurity Resiliency Survey. 2019.
[5] Ebenda.
[6] Wikipedia. Ashley Madison data breach. April 2019.
[7] Ponemon Institute. Cost of a Data Breach Study 2018.
[8] Malwarebytes. Cybersecurity Resiliency Survey. 2019.
[9] Ponemon Institute. The Third Annual Study on the Cyber Resilient Organization. 2018.
[10] Ebenda.
[11] SANS. The Definition of SOC-cess? SANS 2018 Security Operations Center Survey. August 2018.
[12] Ponemon Institute. Cost of a Data Breach Study 2018.
[13] Ponemon Institute. 2018 Cost of Data Breach Study. Juli 2018.
[14] Malwarebytes. Cybersecurity Resiliency Survey. 2019.
[15] Ebenda.
[16] SANS Institute. 2019 SANS Automation & Integration Survey. März 2019.
[17] Ponemon Institute. 2018 Cost of Data Breach Study. Juli 2018.
[18] Ebenda.