Magazine

„Cybersicherheit trägt heute mehr denn je Verantwortung dafür, dass die Zukunft der Arbeit erfolgreich ist.“

Die Zukunft der Arbeit

Edition

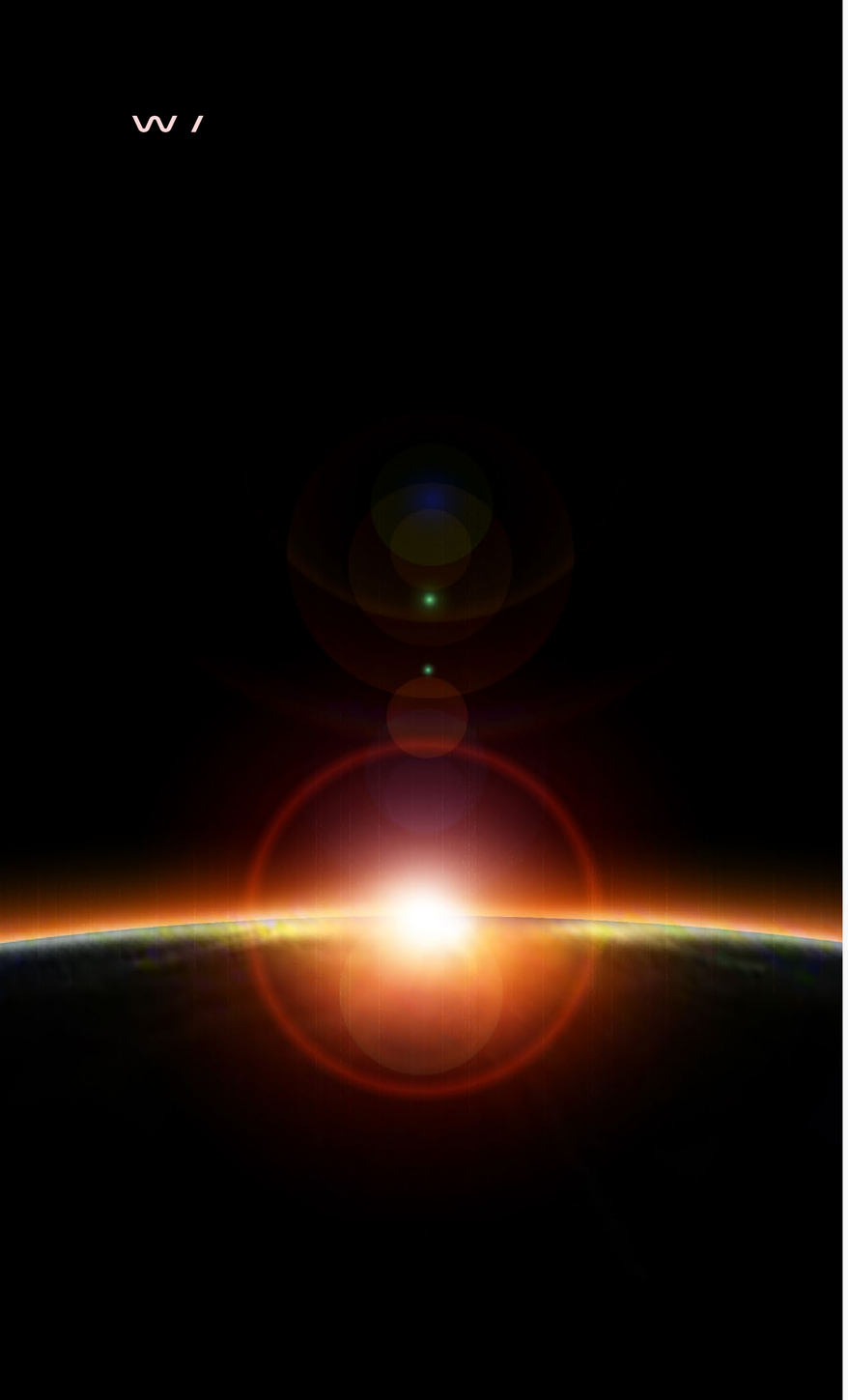
Eine resiliente digitale Zukunft schaffen

Interview mit WithSecure™-CISO Erka Koivunen

Für mehr Sichtbarkeit sorgen

Ein reibungslos hybrides Arbeitsmodell

WITH secure



Eine resiliente digitale Zukunft schaffen

Die Rückkehr ins Büro dominiert derzeit die Diskussion über die Zukunft der Arbeit. Mittlerweile haben sich von CEOs und Bankdirektoren bis zu Marktanalysten und LinkedIn-Influencern fast alle dazu geäußert, wie, wann und ob die „große Rückkehr“ stattfinden soll.

Ein Großteil der Medienberichterstattung und der Forschung konzentriert sich auf die Differenzen zwischen den Plänen der Firmen und den Erwartungen der Beschäftigten. Laut Gartner sind die Ansprüche an Telearbeit bei 75 % der Wissensarbeiterinnen und -arbeiter gestiegen; 39 % der Beschäftigten würden ihren Arbeitsplatz verlassen, wenn sie zu einem reinen Vor-Ort-Modell zurückkehren müssten.

Unabhängig davon, wie die neue Struktur konkret aussehen wird – und es scheint sicher, dass ein Hybridmodell die nächste, vielleicht sogar die letzte Stufe in der Evolution der Arbeit sein wird –, bietet die aktuelle Situation den Unternehmen eine Chance, ihre digitale Strategie neu am Konzept der Resilienz auszurichten.

Wir definieren Cyberresilienz als die Fähigkeit einer Organisation, sich gegen ernsthafte Bedrohungen ihrer IT-Infrastruktur zu schützen, aber auch Kompromittierungen zu erkennen und darauf zu reagieren, sodass der Betrieb rasch wieder aufgenommen werden kann.

Für die Sicherheitsbranche ist Cyberresilienz nichts Neues, aber auch darüber hinaus setzt sich das Konzept jetzt durch. Einer Ponemon-Institute-Umfrage unter mehr als 3400 IT-Fachleuten zufolge ist die Zahl der Unternehmen, die sich ein hohes Maß an Cyberresilienz zuschreiben, 2015 bis 2020 von 35 % auf 53 % gestiegen.

Ein Teil dieses Bewusstseinswandels ist auf die leidige Tatsache zurückzuführen, dass die Angreifer schneller auf die Pandemie reagiert haben als die meisten Unternehmen. Eine Umfrage von Cisco zeigt, dass 61 % der Befragten seit Corona einen Anstieg der Cyberbedrohungen um 25 % verzeichnet haben, wobei kleine Unternehmen am heftigsten betroffen sind.

Unterm Strich bedeutet das, dass die Cybersicherheit heute mehr denn je Verantwortung dafür trägt, dass die Zukunft der Arbeit erfolgreich ist. Für 85 % der Unternehmen ist Cybersicherheit heute sehr wichtig oder wichtiger als vor der Pandemie. CISOs und IT-Entscheider müssen sicherstellen, dass ihre Unternehmen auf Unterbrechungen reagieren können und sich davon erholen, bevor die Geschäftsfortführung ernsthaft gefährdet ist.

In dieser Ausgabe befassen wir uns mit der Frage, wie CISOs diesen Übergang bewältigen und welche Security-Ziele 2022 Vorrang haben.

Interview mit Erka Koivunen

Erka Koivunen ist unser hauseigener CISO, er leitet seit fünf Jahren die Abteilung für interne Sicherheit bei WithSecure™. Im Folgenden gibt er darüber Auskunft, wie CISOs die Herausforderungen der neuen Arbeitswelten konzeptuell fassen und angehen sollten.

F: Erka, wie hat sich deine Arbeitsweise und deine Art, Sicherheitsrisiken zu bewerten, durch die vermehrte Telearbeit geändert?

E. K.: Als auf einmal weltweit alle zur Telearbeit gezwungen waren, mussten die Unternehmen mit einer Netzwerk- und IT-Infrastruktur ohne Zero-Trust-Philosophie am meisten ändern. Bei ihnen versagten die bestehenden Sicherheitskontrollen komplett, und wahrscheinlich hatten sie auch keine Zeit, ein entsprechendes System einzurichten, sodass sie extrem exponiert waren. Zugleich mussten sie für ihre Belegschaft unbedingt ein provisorisches Fernzugriffssystem schaffen.

Das zwang alle dazu, sich schlagartig auf neue Arten von Risiken einzulassen. Eine der ersten Entscheidungen, die die CISOs treffen mussten, war zum Beispiel die Frage, ob und welche Art von Überwachung sie einführen sollten. Im alten Paradigma brachte die Bürogestaltung es mit sich, dass die Vorgesetzten einen gewissen Überblick darüber hatten, was ihre Leute taten und wo sie waren, und das war so etwas wie die grundlegende Sicherheitskontrolle. In Remote-Umgebungen dagegen können die Beschäftigten tagelang verschwinden, ohne dass es jemand merkt. Entweder musste man dieses Risiko in Kauf nehmen oder einen Weg finden, es auszugleichen.

F: Wie reagieren CISOs am besten auf diese neuen Risiken?

E. K.: Also, einen Zero-Trust-Ansatz einzuführen, ist ein sehr hilfreicher erster Schritt. Es bedeutet, ein System einzurichten, das mithilfe einer Reihe von Faktoren Vertrauen aufbaut. Eine ordentliche Einrichtung verknüpft das Gerät, die Client-Anwendung, die Benutzeridentität, die Sitzung, den Dienst und das Netz miteinander. Das System unter der Haube überprüft dann ständig alle diese Variablen und stellt damit sicher, dass der Benutzer auch derjenige ist, der er vorgibt, zu sein.

F: Welche Art von Sicherheitsergebnissen sollten CISOs vor diesem Hintergrund 2022 anvisieren?

E. K.: Sichtbarkeit und Kontextbewusstsein sind für das Funktionieren eines Zero-Trust-Ansatzes unerlässlich. Sie müssen überprüfen können, ob der Endpunkt, von dem aus auf Firmenressourcen zugegriffen wird, und das Benutzerverhalten mit den Sicherheitszielen übereinstimmen.

Bei der Telearbeit war es anfangs so, dass die Beschäftigten von unterschiedlichen Orten aus eine Verbindung herstellten – von ihrem Heimnetzwerk, über das WLAN des Nachbarn oder aus einem Hotel am anderen Ende der Welt, in dem sie gelandet waren. Zuvor konnten die CISOs vernünftigerweise von einer sicheren Netzwerkverbindung ausgehen, aber das war jetzt nicht mehr der Fall. Im neuen Szenario ist der Ansatz sinnvoll, sich mit einer Kombination aus EDR (Endpoint Detection and Response) und EPP (Endpoint Protection Platform) auf den Endpunktschutz zu konzentrieren, weil man damit eine gewisse Tiefe und Nuancierung der Anomaliewarnungen erreicht. Wenn jemand, der sich mit den Zugangsdaten eines Mitarbeiters anmeldet oder Rechenleistung und Verbindungen Ihres Produktivsystems nutzt, anfängt, sich seltsam zu verhalten, dann kann EDR mit großer Sicherheit sagen, ob es sich um den Benutzer selbst handelt oder um jemanden, der sich für ihn ausgibt.

Die Sicherheitsteams können auf dieser Grundlage noch ein weiteres, sekundäres Ziel ins Auge fassen, nämlich die Kultivierung einer humanzentrierten Sicherheit. Wenn Sie an das Stereotyp des klassischen Security-Managers denken, der keine Menschen mag, weil er immer nach Verrätern und Betrügern Ausschau hält und Beweise für seine etwas paranoide Weltsicht sammelt, dann wird rasch klar, wie anders der EDR-Ansatz ist: EDR kann feststellen, ob es sich um einen Prozess handelt, der von einer bekannten Malware-Entität gestartet wurde oder zu einem bekannten Angriffsmuster gehört – und nicht etwa von einer Person.

Wenn EDR feststellt, dass der Benutzer selbst ein Opfer und kein böswilliger Täter ist, dann können wir ihn als Verbündeten mit ins Boot holen. Man sollte nicht pauschal alle wie feindliche Akteure behandeln, im Gegenteil – es ist für Sicherheitsbeauftragte sogar recht nützlich, wenn sie mit der Belegschaft auf gutem Fuß stehen.

F: Danke, Erka. Mehr Sichtbarkeit und ein personalfreundlicherer Ansatz sind großartige Ziele. Aber wie lässt sich das auf eine Arbeitswelt übertragen, die weitgehend von Cloud-Apps abhängt? Welche zusätzlichen Sicherheitsmaßnahmen müssen CISOs für diese Anwendungen erwägen?

E. K.: Im Idealfall sind Sie in der Lage, Ihre Reaktionsmaßnahmen zu orchestrieren, verfügen also über einen Erkennungsmechanismus, der sowohl Endpunkte als auch Cloud-Instanzen und Anwendungslogik nahtlos überwacht und feststellen kann, ob auf all diesen Schauplätzen ein Angreifer unterwegs ist. Leider sind viele Sicherheitsprodukte derzeit noch Silos. Das bedeutet: Sie müssen von Hand überprüfen, was in Ihrer Salesforce-Sicherheitslösung passiert, und müssen dies dann mit Ihrer Microsoft-Sicherheitslösung und der EDR-Lösung abgleichen, damit Sie ein vollständiges Bild bekommen.

Unser Ziel ist die Orchestrierung über eine einzige Konsole. Aber letztlich kann man Anwendungen erst überwachen, wenn sie überhaupt überwachbar sind. Wenn es keine API für Monitoring und Steuerung gibt, wird das schwierig.

F: Was können Unternehmen sonst noch konkret tun, um sich für das zu rüsten, was bevorsteht, ob es nun eine längere Phase reiner Telearbeit ist oder eine Art von Hybridmodell?

E. K.: WithSecure™ agiert weltweit. Darum war uns schon vor der Komplettumstellung auf Remote Work klar, dass bestimmte Teile des Unternehmens in der Lage sein müssen, ihre Aufgaben unabhängig von ihrer geografischen Position, ihrem topologischen Ort (im Netzwerk) und ihrer Zeitzone zu erfüllen.

Aus diesem Grund hatten wir bereits damit experimentiert, bei bestimmten Teams sämtliche Meetings in Fernkonferenz abzuhalten. Das fühlte sich anfangs etwas künstlich an, hatte aber den Vorteil, dass alle gleichbehandelt wurden und niemand einen Vorteil hatte. Und es hatte zur Folge, dass wir schon wussten, wie wir Netzwerkkapazitäten, Latenzen und die Skalierbarkeit der Dienste planen mussten, damit alle gleichzeitig online sein konnten. Als es dann ernst wurde, brachte das enorme Vorteile mit sich.

Die Lehre daraus ist also, dass man als Organisation beizeiten üben und ausprobieren muss. Im Trainingsmodus kann man Dinge austesten, die im Moment noch gar nicht so dringend erscheinen, und meistens müssen sie auch nicht zu wirklichen Veränderungen führen, aber man kommt so auf neue Wege, die Probleme anzugehen.

F: Und welche Art von Übungen sollten CISOs jetzt angehen?

E. K.: Es ist kein Geheimnis, dass wir uns im Training derzeit auf den Fall vorbereiten, dass unsere internen Systeme ganz oder teilweise unter die Kontrolle von externen, übel gesinnten Akteuren geraten. Sie müssen wissen, welche Schutz- und Segmentierungsmöglichkeiten Sie haben, wie Sie Probleme isolieren können und mit welchen Mitteln Sie nach einem solchen Vorfall wieder auf die Beine kommen.

Wer die Nachrichten über Ransomware-Banden verfolgt hat, weiß, dass darin ein weitverbreitetes Problem seinen ökonomischen Ausdruck findet, nämlich dass Unternehmen nicht in der Lage sind, sich vor Sicherheitsvorfällen zu schützen, sie zu erkennen und darauf zu reagieren.

Mit den Werkzeugen und der Sichtbarkeit, die EDR- und MDR-Lösungen als Managed Services bieten können, kann man viele dieser Schwierigkeiten in den Griff bekommen und das Risiko einer Kompromittierung deutlich senken.

Für mehr Sichtbarkeit sorgen

Um Cyberresilienz zu erreichen, müssen Sicherheitsverantwortliche zunächst wissen, womit sie überhaupt arbeiten. Das Monitoring der Remote-Verbindungen ist enorm wichtig, wenn man Schadaktivitäten sichtbar machen und die damit verbundenen Sicherheitsrisiken eindämmen will. Die Forschung zeigt allerdings, dass dieses Monitoring leichter gesagt als getan ist.

Derzeit sollte es verstärkt darum gehen, die Netzwerktransparenz zu verbessern, die Remote-Beschäftigten mit sicheren, vorkonfigurierten und kontrollierten Geräten auszustatten und der Belegschaft einfache, integrierte und handhabbare Lern- und Sicherheitstools zu geben.

Für viele Unternehmen wird dies zusätzliche Investitionen in ihre XDR-Fähigkeiten (Extended Detection and Response) bedeuten. So konstatiert der SWZD-Report „State of IT 2021“, dass der Endpunktschutz derzeit oberste Priorität hat. Das ist nur folgerichtig, denn die wertvollsten Daten der meisten Unternehmen liegen auf den Endgeräten.

Laut der jüngsten WithSecure™-Untersuchung zur Angriffslandschaft haben sich durch den Wechsel zu Telearbeit die Grenzen des Unternehmensnetzwerks exponentiell ausgedehnt – und damit auch die Angriffsfläche. Und noch mehr Daten liegen heute jenseits dieser Grenzen. Hinzu kommt, dass Beschäftigte von außerhalb mit größerer Wahrscheinlichkeit von unsicheren Geräten und Netzwerken aus arbeiten und einen weniger engen Kontakt zu den IT-Sicherheitsteams haben. Diese brauchen darum eine einfache Möglichkeit, Endpunktrisiken zu identifizieren, zu sortieren und schnell darauf zu reagieren. Detection-and-Response-Technologie macht mit einer einzigen Übersicht die gesamte IT-Umgebung und den Sicherheitsstatus sofort sichtbar; sie sorgt für die Sicherheit des Unternehmens und der Daten, weil die Teams damit Angriffe schnell erkennen und unter fachkundiger Anleitung reagieren können.

Genau diese Expertise ist jedoch schwer zu finden. Der Fachkräftemangel im Bereich Cybersicherheit ist hinlänglich bekannt, und Covid-19 hat die Lage noch verschärft. Dass es mehr offene Stellen als qualifizierte Bewerber gibt, ist eine der größten Herausforderungen für Unternehmen, die jetzt Strategien für die Zukunft der Arbeit entwickeln.

In einer Umfrage des Personaldienstleisters Robert Half hat fast ein Drittel (32 %) der CIOs und CTOs angegeben, dass seit der Pandemie IT-Mitarbeiter mit Security-Kompetenzen am schwersten zu finden sind. Und laut Gartner ist der Bedarf bei Stellen im Bereich Informationssicherheit in Großbritannien und den USA seit Beginn der Pandemie sprunghaft gestiegen, in den USA sogar um 65 %.

Viele Unternehmen werden sich bemühen, diese Kompetenzlücke durch Managed Security Services zu schließen. 59 % der von ConnectWise befragten KMU glauben, dass sie in fünf Jahren alle bzw. die meisten ihrer Cybersicherheitsaufgaben ausgelagert haben werden; 49 % sagen, dass sie die verstärkten Sicherheitskompetenzen als einen zusätzlichen Vorteil von Managed Services sehen.

Diese Art der Zusammenarbeit wird für viele Unternehmen von entscheidender Bedeutung sein, denen bewusst ist, wie wichtig es ist, Cyberresilienz ins Zentrum der New-Work-Strategie zu rücken, die aber nicht über die Ressourcen verfügen, um alles selbst zu bewältigen.

Ein reibungslos hybrides Arbeitsmodell

Ein reibungsloses Hybrid-Arbeitsmodell gehört heute wesentlich zu den Aufgaben eines Sicherheitsteams. In der Praxis bedeutet dies, eine sichere Zusammenarbeit zu ermöglichen – was für die meisten Unternehmen auf die Arbeit mit SaaS-Cloud-Anwendungen hinausläuft.

„ Bei jedem Collaboration-Tool, das Sie heute verwenden, ob Microsoft 365, Teams, SharePoint oder Salesforce etc., gehen die Daten in die Cloud, und als Unternehmen müssen Sie darauf achten, wie die Sicherheit dieser Daten gewährleistet wird.“

Juha Högmander, WithSecure™

„Bei jedem Collaboration-Tool, das Sie heute verwenden, ob Microsoft 365, Teams, SharePoint oder Salesforce etc., gehen die Daten in die Cloud, und als Unternehmen müssen Sie darauf achten, wie die Sicherheit dieser Daten gewährleistet wird“, sagt Juha Högmander, Director of Product Management bei WithSecure™.

Am häufigsten wird Microsoft 365 genutzt. Darum hat WithSecure™ in die Allzweck-Sicherheitsplattform WithSecure™ Elements ein Tool für die Sicherheit von Microsoft 365 integriert. Dieser Ansatz, Cloud Security auf einer Plattform mit EPP, EDR, Schwachstellenmanagement etc. zu integrieren, ist laut Högmander die Zukunft: „Mit Elements werden wir eine wachsende Anzahl von Cloud-Anwendungen und -Diensten im Blick behalten“, sagt er.

Der verbesserte Schutz trägt definitiv zu einem reibungsloseren Hybrid-Arbeitsmodell bei. Das gilt mit Blick auf die Beschäftigten, weil sie dann kaum mehr durch einen Klick auf eine Schadmail aus der Bahn zu werfen sind, es gilt aber auch speziell für die Effizienz des Sicherheitsteams.

Angriffsbeispiel

Das folgende Beispiel zeigt Schritt für Schritt, wie integrierte E-Mail-Sicherheit die Security-Leistung des Unternehmens bei einem E-Mail-Angriff verbessert.

Silo-Lösungen (E-Mail + EDR)	WithSecure™ Elements (EDR + MS 365)
1. Ein Benutzer erhält eine Schad-E-Mail; die Silo-Lösung markiert sie zwar als verdächtig, leitet aber wahrscheinlich keine Maßnahmen ein; ein zentraler Log-Eintrag erfolgt nicht.	1. Ein Benutzer erhält eine Schad-E-Mail; der integrierte E-Mail-Schutz markiert sie als verdächtig und zeichnet den Vorgang in der zentralen Konsole auf.
2. Der Angreifer übernimmt per C&C-den Rechner; die Silo-EDR erkennt dies und warnt, das Security-Team reagiert.	2. Der Angreifer übernimmt per C&C-den Rechner; die integrierte EDR erkennt dies und warnt, das Security-Team reagiert.
3. Der Zusammenhang mit der ursprünglichen E-Mail bleibt unerkannt, es sei denn, das Sicherheitsteam erinnert sich von selbst daran und überprüft das.	3. Die Ursache wird in der zentralen Konsole automatisch hervo-rgehoben, das Sec-Team kann die E-Mail-Regeln anpassen und damit diese Sorte Mail für alle Beschäftigten blockieren.

„XDR heißt, dass Sie Daten aus verschiedenen Cloud-Quellen sammeln und kombinieren, sodass sich ein vollständiges Bild ergibt und Sie entsprechend reagieren können“, sagt Högmander. Der integrierte E-Mail-Schutz ist nur ein Beispiel dafür, wie das mit WithSecure™ Elements in der Praxis funktioniert.

Situationsbewusstsein

Sichtbarkeit ist ein zentrales Thema dieser Ausgabe, und das aus gutem Grund. Wer einen Angreifer stoppen will, muss zuerst einmal wissen, dass der Angreifer da ist. Der nächste Schritt besteht darin, dass das Sicherheitsteam ein Situationsbewusstsein entwickelt, damit es das, was es sieht, auch in seiner Bedeutung erfasst. Högmander von WithSecure™ beschreibt das so: „Wenn man die Art des Angriffs kennt, weiß man auch, welche Art von Verteidigung man braucht."

Ein Situationsbewusstsein zu entwickeln, ist in Wirklichkeit jedoch komplexer. Es erfordert Kenntnis von der Situation weltweit und von der Bedrohungslage, damit eine angemessene Alarmstufe festgelegt werden kann. Wenn z. B. ein Ransomware-Angriff stattfindet und viele Unternehmen eines vertikalen Marktes betroffen sind, dann können andere Unternehmen aus diesem Branchensegment darauf aufmerksam gemacht werden. Allerdings wissen sie dann nur, was in den Nachrichten steht, kennen aber vermutlich nicht die Details und wissen nicht, welche Maßnahmen sie ergreifen müssen, um sich zu schützen.

Högmander erklärt, wie WithSecure™ Elements dieses Problem angeht: „Wenn sich die Situation in der Bedrohungslandschaft ändert, erhöht Elements das Sicherheitslevel. Ein ungeschütztes Gerät, das vorher gelb markiert war, wird dann orange, und falls sich zielgenaue Ransomware verbreitet, wird es sofort rot."

Auf diese Weise können Unternehmen gemeinsam ein viel stärker differenziertes Situationsbewusstsein entwickeln, als sie es alleine je könnten. „Wir sammeln alle Daten zu Schwachstellen und verdächtigen Ereignissen aus der Umgebung des Kunden, einschließlich der Daten aus Geräten und Cloud-Anwendungen, und kombinieren dies mit unserer Analyse der Benutzerinteraktion mit dem IT-System – und wir wissen, welches Risiko in diesem Moment besteht. Dann kann vor allem das richtige Risiko priorisiert und beseitigt werden", fasst Högmander zusammen.

Aus diesem Situationsbewusstsein heraus kann man geeignete Maßnahmen ergreifen. Elements bietet bereits Reaktionen für alle fortschrittlichen Fälle an, die EDR erkennt, und die Entwicklung geht dahin, dass die Lösung am Ende die Reaktionen über alle Bereiche hinweg koordinieren kann. Der oben dargestellte E-Mail-Angriff ist bereits ein Beispiel für eine Reaktionsmaßnahme, die in einer anderen Domäne als die Erkennung erfolgt: Erkennung in der EDR-Lösung, Reaktion in der E-Mail-Lösung.

Neben besserer Sichtbarkeit und einem reibungslosen Übergang zu einem hybriden Arbeitsmodell wird die Entwicklung eines starken Situationsbewusstseins ein wichtiger Schritt für Unternehmen sein, die 2022 und darüber hinaus ihre Reaktionsfähigkeit und damit ihre Cyberresilienz verbessern wollen.

Über WithSecure

WithSecure™ ist der zuverlässige Partner für Cybersicherheit. IT-Dienstleister, Managed Security Services Provider und andere Unternehmen vertrauen WithSecure™ – wie auch große Finanzinstitute, Industrieunternehmen und führende Kommunikations- und Technologieanbieter. Mit seinem ergebnisorientierten Ansatz der Cybersicherheit hilft der finnische Sicherheitsanbieter Unternehmen dabei, die Sicherheit in Relation zu den Betriebsabläufen zu setzen und Prozesse zu sichern sowie Betriebsunterbrechungen vorzubeugen. WithSecure™ nennt diesen Ansatz „Outcome-based Cyber Security". KI-gesteuerte Sicherheitsmaßnahmen sichern Endpoints und die Zusammenarbeit in der Cloud mit intelligenten Erkennungs- und Reaktionsmechanismen. Die Detection & Response-Experten von WithSecure™ identifizieren Geschäftsrisiken, indem sie proaktiv nach Bedrohungen suchen und bereits laufende Angriffe abwehren – dabei arbeiten sie eng mit Instituten, großen Unternehmen und innovativen Tech-Firmen zusammen. Sie haben mehr als 30 Jahre Erfahrung in der Entwicklung von Technologien, die sich an den Bedürfnissen der Unternehmen orientieren. Das Portfolio von WithSecure™ eröffnet durch flexible Vertriebsmodelle die Möglichkeit, gemeinsam mit Partnern zu wachsen.

WithSecure™ ist Teil der 1988 gegründeten F-Secure Corporation, die an der NASDAQ OMX Helsinki Ltd. gelistet ist.

W / T H
secure