kaspersky BRING ON THE FUTURE

Cybersicherheit für die Zeit nach Covid-19

Die Herausforderungen der Cybersicherheit für Unternehmen in 2020er Jahren meistern

Fernarbeit hat sich während der Pandemie zu einer Erfolgsgeschichte entwickelt, deren eigentliche Helden, nämlich die IT-Abteilungen, wenig Beachtung fanden. Unternehmen, die nicht auf direkten Kundenkontakt angewiesen waren, haben Lockdown und Restriktionen nicht nur gut überstanden, sondern konnten sogar Gewinn daraus ziehen, weil Ihre Mitarbeiter effektiv und sicher von zu Hause aus arbeiten konnten, auf beruflichen oder privaten Laptops, PCs und anderen Geräten.

Es hat sich gezeigt, dass das Arbeiten von Zuhause einige Vorteile bietet, darunter mehr Produktivität, geringere Fehlzeiten, bessere Mitarbeiterbindung und geringere Kosten für Büroflächen. Und auch wenn bei einigen Mitarbeitern die anfängliche Euphorie über den Dauerarbeitsplatz im eigenen Wohnzimmer mittlerweile abgenommen hat, kann man für die Zukunft wohl davon ausgehen, dass sich eine gewisse Mischung aus Heim- und Büroarbeit zur Norm entwickeln wird.

Eine von Kaspersky in Auftrag gegebene Studie[1] ergab:

- 74 % der Mitarbeiter möchten zumindest teilweise nicht mehr zur Arbeitsplatzdynamik von gestern zurückkehren.
- 39 % der Mitarbeiter sind bereit, die traditionell festgeschriebenen Bürozeiten von 9 bis 17 Uhr aufzugeben.
- 34 % möchten nicht mehr an einem festen Büroarbeitsplatz arbeiten.
- 32 % möchten die Fünf-Tage-Woche überdenken.

„Die Kosten für Cyberkriminalität könnten sich durch den Ausbruch des Coronavirus verdoppeln."

Cybersecurity Ventures, July 2020

Die Geschichte der Cybersicherheit

Und wie ist es der Cybersicherheit ergangen während dieses drastischen Wandels in der Arbeitspraxis? Bei allen geschäftlichen Vorteilen der Fernarbeit, gibt es durchaus auch Nachteile. Einer davon ist die erhöhte Anfälligkeit von remote installierten und betriebenen Endpoints gegenüber Angriffen. Und mittelbar ist dadurch auch die gesamte Unternehmensinfrastruktur gefährdet.

Kurz gesagt: Für Cyberkriminelle sind Remote-Arbeitsplätze ein gefundenes Fressen.

- Vor der Pandemie gingen im US-amerikanischen Internet Crime Complaint Center täglich etwa 1.000 Beschwerden über Cyberkriminalität ein. Mittlerweile sind es zwischen 3.000 und 4.000 pro Tag[2].
- Einem Bericht von Interpol[3] im August 2020 zufolge gab es „während Covid-19 eine alarmierende Zahl von Cyberangriffen".
- Die Zahl der Phishing- und Remote-Angriffe hat Spitzenwerte erreicht, wobei laut Cybersecurity Ventures[4], einem führenden Magazin der Branche, Angestellte im Home Office es mit der Sicherheit eher lax halten.

Welches sind die größten Sicherheitsprobleme?

- Remote-Endpoints werden nicht mehr über ein Unternehmens-LAN betrieben. Vielmehr geht man über den heimischen Router ins Internet oder nutzt ungesicherte WLAN-Zugänge an öffentlichen Plätzen. Das macht Endpoints anfälliger für Man-in-the-Middle-Angriffe.

[1] Securing the Future of Work, Kaspersky, 2020

[2] Combatting Cybercrime During COVID-19, Aspen Digital, 2020

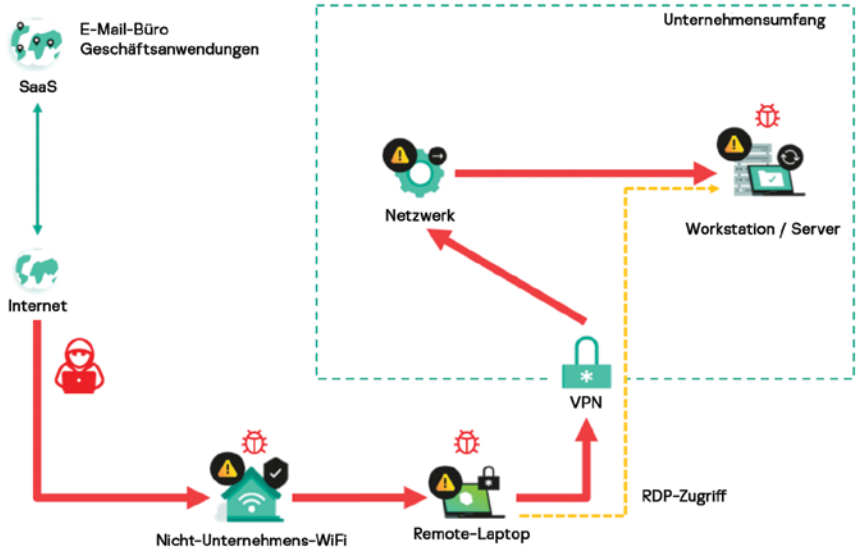
[3] Bericht von INTERPOL weist auf eine alarmierende Zahl von Cyberangriffen während der Pandemie hin, INTERPOL, August 2020

- Von Unternehmen bereitgestellte Geräte werden oft als Heim-PCs verwendet, um private E-Mails zu lesen, den Hobbys nachzugehen usw. Und wer allein zu Hause arbeitet statt im geschäftigen Büro, ist eher versucht, fragwürdige und potentiell gefährliche Webseiten am beruflichen Laptop zu öffnen, wodurch die Geräte einem noch größeren Risiko ausgesetzt sind.
- Die Verwendung eigener privater Geräte verschärft die Situation noch zusätzlich. Denn damit ist der Nutzer auch der Administrator, d. h. Sie haben wenig oder oder gar keine Kontrolle darüber, welche Art von Schutz auf den Geräten installiert ist, die sich mit Ihrer Unternehmensinfrastruktur verbinden, oder wie sie konfiguriert sind.

Ist der Endpoint einmal befallen, kann der Nutzer nicht arbeiten, wertvolle, auf dem Gerät gespeicherte Daten sind gefährdet und die Identität eines Benutzers kann genutzt werden, um Angriffe auf Ihre Kunden zu lancieren, z. B. über dessen geschäftliches E-Mail-Konto. Aber was noch viel schwerwiegender ist: Wenn Angreifer über einen einzelnen Endpoint in Ihren Perimeter eindringen, können sie sich horizontal über das gesamte Netzwerk ausbreiten, sich dort festsetzen, Malware aktivieren und die Kontrolle über Ihre Systeme übernehmen. Das ist zumindest die standardmäßige Vorgehensweise selbst bei den komplexesten, raffiniertesten und größten (und teuersten) Angriffen auf Unternehmen – zum Einstieg genügte ein einziges Gerät.

VPNs oder RDP bieten eine sichere Kommunikation zwischen Remote-Endpoints und Ihrem Netzwerk. Aber auch sie sind Risiken ausgesetzt. Gestohlene Anmeldedaten – entweder über Brute Force-Angriffe, Phishing oder Social Engineering – kann im Darknet für wenige Dollar jeder bekommen, der ein Interesse daran hat, Sie anzugreifen. Ebenso kann ein Remote Access-Trojaner (RAT) auf einem Endpoint installiert werden, ohne dass Sie oder der Nutzer davon etwas merken.

Jeder dieser Einstiegspunkte kann genutzt werden, um Ransomware zu installieren, illegale Finanzoperationen durchzuführen, Daten zu stehlen – oder sich einfach nur Zugang zu Ihren Systemen zu verschaffen und diesen Zugang online an den Meistbietenden zu verkaufen.



Man darf auch nicht vergessen, dass jedes remote eingesetzte Gerät, das ins Büro gebracht und direkt an das Firmennetzwerk angeschlossen wird, der darauf befindlichen Malware einen weiteren Zugangsweg direkt in Ihre Systeme eröffnet.

Was tun?

Wie so häufig in der Cybersicherheit, besteht die Lösung in einem vielschichtigen Ansatz mit mehreren Abwehrstufen und einem besonderem Augenmerk auf diese anfälligen Remote-Endpoints.

Sie können zum Beispiel folgende Maßnahmen ergreifen:

Auf VPN/RDP-Ebene

Seit Anfang März hat die Zahl der Bruteforce.Generic.RDP-Angriffe weltweit dramatisch zugelegt[4]

- **MFA implementieren**: Multi-Faktor-Authentifizierung (z. B. Passwort + Sicherheitstoken) für den Zugang von Endpoints zum VPN.
- **RDP-Zugriff beschränken**: auf IP-Adressen, die vom VPN des Unternehmens kommen.
- Dem Angreifer das Leben schwer machen, indem man **eine nicht standardmäßige RDP-Portnummer verwendet** (statt 3389).
- Ziehen Sie in Erwägung, **jeglichen Webverkehr über einen gesicherten Proxyserver zu leiten** – vorausgesetzt, Sie verfügen über die entsprechenden Ressourcen und Kapazitäten, was natürlich nicht bei vielen Unternehmen der Fall sein wird.
- **Beschränken Sie den Funktionsumfang und die Programme, auf die** über VPN oder RDP zugegriffen werden kann. Die dafür erforderliche Konfigurationsarbeit nimmt einige Zeit in Anspruch, sollte es aber wert sein, wenn dieser Ansatz in Ihrem Unternehmen Akzeptanz findet.
- **Eventuell können Sie auch Ihren Perimeterschutz aktualisieren** – Sicherheitslösungen für E-Mail-Server und Web-Gateways, die die Mehrzahl der Bedrohungen blockieren, bevor sie die Endpoint-Ebene erreichen, sind grundsätzlich eine gute Investition.

Auf der Ebene der Workstation

Zugriffskontrollen auf Webseiten und Anwendungen, die für die eigentliche Tätigkeit nicht relevant sind, haben den zusätzlichen Vorteil, dass die Nutzung sozialer Medien, das Surfen im Internet, Online-Shopping und andere zeitraubende Aktivitäten während der Arbeitszeit reduziert werden und so die Produktivität gesteigert wird – eine in der Wirtschaft oft geäußerte Sorge, wenn es um Fernarbeit geht.

Reduzieren Sie die Angriffsfläche durch Systemhärtung. Begrenzen oder unterbinden Sie den Zugriff von Workstations auf bestimmte Webseiten bzw. blockieren Sie die Ausführung bestimmter Programme über Positiv- und Negativlisten. Sie können auch die Umsetzung einer „Default Deny"-Richtlinie in Erwägung ziehen, bei der nur bestimmte arbeitsbezogene und systemeigene Programme auf dem Gerät ausgeführt werden können. Damit werden Sie sich keine Freunde machen bei den Mitarbeitern, die ihre beruflichen Geräte auch privat nutzen, aber als Sicherheitsansatz ist diese Maßnahme sehr wirkungsvoll.

Schützen Sie Unternehmensdaten durch Verschlüsselung. Geräte, die nicht fest im Büro installiert sind, können verloren gehen. Dann müssen Sie sicher sein können, dass alle vertraulichen Daten darauf für Außenstehende unantastbar und unbrauchbar sind.

Beim Patching immer am Ball bleiben. Es mag banal klingen, aber zeitnahes, priorisiertes Patching ist unverzichtbar. Die Ausnutzung von Schwachstellen in gängigen Programmen ist immer noch der mit Abstand beliebteste illegale Einstiegspunkt in Unternehmenssysteme.

Erkennen Sie verdächtige Aktivitäten in Endpoints mithilfe einer Anomaliekontrolle. Ist das sicher, oder kann das weg? Verhält sich eine Remote-Workstation ungewöhnlich? Ihre Sicherheitslösung muss so etwas automatisch erkennen und schnell reagieren können.

Nutzen Sie robuste Erkennungs- und Beseitigungstools. Es ist allgemein bekannt, dass EDR (Endpoint Detection and Response) in Kombination mit einer soliden EPP-Plattform (Endpoint Protection Platform) für einen effektiven Endpoint-Schutz unverzichtbar ist, vor allem wenn man es mit versteckten Cyberangriffen zu tun hat. Das muss nicht viel Zeit in Anspruch nehmen – automatisierte Erkennungen können in vielen Fällen durch automatisierte Abwehrmaßnahmen gekontert werden. Ihr Team muss nur eingreifen, wenn Ihre Lösung ein ernsthaftes Problem entdeckt, um das Sie sich selbst kümmern müssen.

Und wer soll das nun alles machen?

Die Beschäftigung in diesem Bereich muss weltweit um etwa 89 % zunehmen, damit der erwartete Bedarf gedeckt werden kann.[5]

Gute Ratschläge zu geben, ist immer einfacher als sie umzusetzen, dessen sind wir uns bewusst. Insbesondere wenn diese wenig beachteten Helden der Pandemie, die dafür benötigt werden - IT-Fachleute und IT-Sicherheitsexperten so schwer zu bekommen sind. Viele IT-Abteilungen sind derzeit meist unterbesetzt, schlichtweg weil Mitarbeiter für die IT-Sicherheit so schwer zu finden (und zu halten) sind.

In einer Zeit, in der Fernarbeit oder eine Mischung aus Heim- und Büroarbeit, die Zukunft zu sein scheint, mit all den zusätzlichen Problemen für die IT, die das mit sich bringt, versuchen Cyberkriminelle jede sich bietende Chance voll auszunutzen. Daher kommt es für Sie entscheidend darauf an, aus den verfügbaren Mannstunden in Ihrer IT-Sicherheitsabteilung das Maximum herauszuholen.

[4] Remote spring: The Rise of RDP Bruteforce Attacks, Kaspersky, 2020
[5] (ISC)2 Studie zu Mitarbeitern in der Cybersicherheit, (ISC)2, 2020

Automatisierung

Die Lösung besteht größtenteils in der Automatisierung. Viele der oben aufgeführten Aktivitäten – Anomaliekontrolle, Patching sowie andere Elemente zur Erkennung und Systemhärtung – sind dank der Entwicklungen im Bereich des maschinellen Lernens und der Datensammlung komplett oder größtenteils automatisierbar. Darin eingeschlossen sind auch einige fortschrittlichere Prozesse zur Ursachenanalyse und Abwehr. Ein Großteil der schwierigeren Aufgaben sollte also von Ihrer Sicherheitslösung statt von Ihnen und Ihrem Team erledigt werden.

Integration

Die Entscheidung für ein einzelnes integriertes Sicherheitssystem kann ebenfalls viel Zeit sparen. Ein Einzelsatz von Richtlinien, der von einer zentralen Konsole über alle Bereiche des Systems bereitgestellt wird, ist effizienter und senkt das Risiko von administrativen Fehlern. Man sollte sich also gut überlegen, ob man tatsächlich in eines dieser neuen, „punktgenauen" Produkte investiert, die allesamt eine eigene Konsole mitbringen. Denn das kann Zeit und Ressourcen verschlingen, ohne dass es einen Vorteil bringt.

Weniger Warnmeldungen

Wahrscheinlich verbringt auch Ihr Sicherheitsteam viel Zeit damit, routinemäßigen Warnhinweisen nachzugehen, statt sich auf die gefährlicheren versteckten Bedrohungen zu konzentrieren. Das könnte sich ändern, wenn Sie sich jetzt für die EPP-Plattform als Basis entscheiden. Grundlegende Funktionen wie Systemhärtung, effizientes Patching und automatisierte Prävention sorgen für spürbar weniger Warnhinweise, mit denen sich Ihr viel beschäftigtes Team auseinandersetzen muss. Und Sie haben das Recht, von Ihrer Sicherheitslösung eine Fehlalarmrate von nahezu Null zu erwarten. Denn damit sollte Ihr Team nun wirklich nicht seine Zeit verschwenden.

Managed Security-Ansatz

Jetzt ist der Zeitpunkt, um eine Managed Security-Lösung anzusprechen. MDR (Managed Detection and Response) wird derzeit von zahlreichen unter Druck arbeitenden IT-Abteilungen eingeführt. Wenn Sie zur Bearbeitung der schwierigsten Aspekte Ihrer Sicherheit und zur Unterstützung Ihres IT-Sicherheitsteams einen fachkundigen Dritten hinzuziehen, kann das viele Vorteile haben. Ein solcher Anbieter sollte über ausreichend Bandbreite verfügen, um Sicherheitsüberwachung rund um die Uhr anzubieten, aber auch über das Expertenwissen, um Aufgaben wie fortschrittliche Ursachenanalyse, Threat Hunting und sogar geführte und Remote-Abwehrszenarien zu erledigen, sowie über die Ressourcen und das technische Fachwissen, um auf Ihre wachsenden oder schwankenden Anforderungen ganz nach Bedarf eingehen zu können. So oder so kann sich die Beschäftigung eines zuverlässigen Dritten, der Ihnen zumindest einen Teil der Arbeitslast abnimmt, als solide Investition erweisen.

„Wenn sich Mitarbeiter im Home Office nicht disziplinieren und Unternehmen Ihren Angestellten nicht Schulungen für mehr Sicherheitsbewusstsein unter besonderer Berücksichtigung der Bedrohung durch die Heimarbeit anbieten, dann könnten sich die weltweiten Kosten für Schäden durch Cyberkriminalität bis zum Ende dieses Jahres verdoppeln."

Steve Morgan,
Gründer von Cybersecurity Ventures und
Chefredakteur des Cybercrime Magazine

Bewusstsein für Cybersicherheit als Grundlage

Eine Unternehmenskultur, in der Nutzer ein Bewusstsein für Bedrohungen entwickelt haben, über praktische Kompetenzen verfügen, um Gefahren für die Infrastruktur durch bloße Nachlässigkeit oder Unwissen zu vermeiden, und Cyberhygiene allen zur zweiten Natur geworden ist, führt unweigerlich dazu, dass die Arbeitsbelastung des IT-Teams stetig abnimmt. Allgemeines Cyberbewusstsein, eine Kultur des cybersicheren Verhaltens innerhalb der Organisation sowie grundlegende Kompetenzen im Bereich der Cybersicherheit sind der Schlüssel zur Reduzierung der Angriffsfläche und der Zahl der Vorfälle. Organisationen tun sich oft schwer, die richtigen Tools und Methoden für effektive Mitarbeiterschulungen zu finden. Und diese selbst zu erstellen, ist komplex und zeitaufwändig. Um das Sicherheitsbewusstsein zu schärfen, braucht es das richtige Schulungsprogramm für Cybersicherheit – mit einem Schulungsansatz, der die neuesten Techniken und Technologien für die Erwachsenenbildung berücksichtigt. Und der, was noch viel wichtiger ist, relevante und aktuelle Inhalte vermittelt.

Ein zufriedenes, motiviertes IT-Team

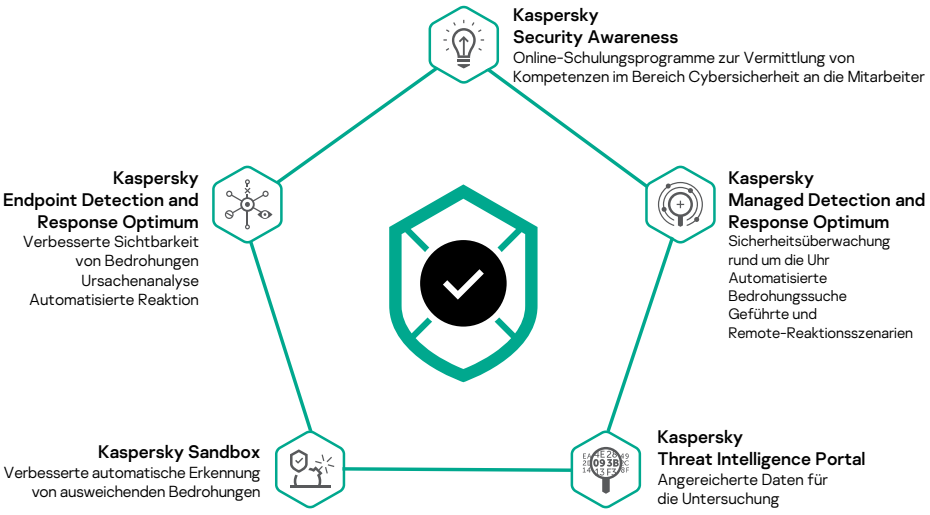
Sicherheitsexperten ist es verständlicherweise ein Graus, ihre Zeit mit langweiligen Routinearbeiten zu vergeuden. Wenn man ihnen also den Raum gibt, sich mit echten Herausforderungen zu befassen, werden Sie mehr Spaß an der Arbeit haben und besser zu halten sein. Was bedeutet, dass Sie es sich leisten können, in die Weiterbildung Ihres Teams zu investieren (vor allem, da es jetzt die Zeit dafür hat), und nicht mehr Gefahr laufen, dass Ihre Experten abgeworben werden – eine Ausgangslage, in der Sie nur gewinnen können.

Unser Angebot

Die Veränderungen in der Informationstechnologie (IT) hat die bestehenden Verfahren in der Cybersicherheit geschwächt und deren zeitnahe Einführung zu einer Herausforderung gemacht. Gleichzeitig ebnet die Cybersicherheit den Weg zu neu entstehende Anwendungsmöglichkeiten digitaler Services und schafft so eine Gelegenheit, den Wandel voranzutreiben.[6]

Ob Sie sich nun für firmenintern, managed oder beides entscheiden, die größte Zeit- und Kostenersparnis erzielen Sie, wenn Sie sich für einen einzelnen Anbieter entscheiden – und zwar einen, der eine komplette mehrstufige EPP/EDR-Plattform und vieles andere mehr zu bieten hat. Das bedeutet auch, dass Sie sich nach einer Lösung umschauen müssen, die langfristig mit Ihnen mitwächst, damit Sie sich später nicht mit zugekauften, übergestülpten Produkten mit eigenen Konsolen und speziellem Schulungsbedarf abmühen müssen.

Kaspersky Optimum Security unterstützt Ihr wachsendes IT-Sicherheitsteam bei der Bewältigung der Herausforderungen, die sich aus gemischte Arbeitsumgebungen ergeben, mit skalierbaren, leicht zu verwaltenden Endpoint-Schutzfunktionen.



Wir bieten Ihnen eine mehrstufige Endpoint-Sicherheitslösung, die hochgradig automatisiert und vollständig skalierbar ist sowie auf dem zuverlässigen Fundament einer preisgekrönten EPP-Plattform aufbaut. Das alles untermauert durch hervorragende MDR-Expertise, Kompetenzen und Schulungen zum Sicherheitsbewusstsein und natürlich durch unseren hochqualifizierten engagierten Support.

Wie Kaspersky Optimum Security Ihr Unternehmen vor versteckten Bedrohungen schützt, finden Sie detailliert dargestellt auf der Webseite: http://go.kaspersky.com/DE_optimum.

[6] ENISA Threat landscape – The Year in Review, European Union Agency for Cybersecurity (ENISA), 2020

Cyber Threats News: https://de.securelist.com/
IT Security News: https://www.kaspersky.de/blog/b2b/

www.kaspersky.de