HYBRID BUSINESS NOW

Informationssicherheit im hybriden Arbeitsbereich

Canon

VORWORT

Tim Rawlins, Geschäftsleiter und Senior Adviser, NCC Group

Das Schlimmste der Pandemie scheint hinter uns zu liegen, doch ihre Auswirkungen auf unsere Arbeitsweise werden wahrscheinlich noch über viele Jahre zu spüren sein.

Die meisten Unternehmen haben schon in den ersten Tagen der Lockdowns schnell neue Wege gefunden, um weiterzuarbeiten. Die IT-Teams haben dabei Großes geleistet, denn sie haben es irgendwie geschafft, dass die Mitarbeitenden innerhalb weniger Tage (manchmal sogar in wenigen Stunden) aus der Ferne arbeiten konnten. Darauf kann man wirklich sehr stolz sein!

Aber in der Eile, in der Wege gefunden werden mussten, um den Betrieb aufrechtzuerhalten, wurden Kompromisse eingegangen – insbesondere bei der Informationssicherheit. Im Rückblick muss man sagen, dass die üblichen Regeln und Vorschriften nicht immer eingehalten wurden.

Jetzt, da hybrides Arbeiten für viele zum Alltag geworden ist, **ist es an der Zeit, diese „Sicherheitsschulden" zu begleichen.** Wir müssen die Schwachstellen beheben, die dadurch entstanden sind und (zu Recht) in Kauf genommen wurden, dass es schnell gehen musste, z. B. offene Heim-WLAN-Netzwerke, schwache Passwörter, übereilte Compliance-Praktiken und unverschlüsselter Dateiaustausch.

Es gibt aber auch noch größere, grundlegendere Probleme, mit denen man sich auseinandersetzen muss. Heutzutage ist es schwieriger, die Aktivitäten von Kriminellen in einem Netzwerk aufzudecken, das nicht mehr sauber durch eine leicht zu kontrollierende Büroumgebung abgegrenzt ist. Da das hybride Arbeiten kontinuierlich zunimmt, sind die Grenzen von Netzwerken unscharf geworden, und die Sicherheit jedes Endpunkts – Laptop, Server oder Smartphone – wird immer wichtiger.

Diese veränderte Arbeitspraxis erfordert neue Denk- und Herangehensweisen – sowie die gute altmodische Informationssicherheitshygiene.

SICHERHEIT NEU DENKEN...

Neue Praktiken müssen in Betracht gezogen werden, wie z. B. eine wirksame Netzwerksegmentierung. Dabei wird das interne Netzwerk aufgeteilt, um die wichtigsten Ressourcen besser kontrollieren und schützen zu können. Aufgrund der Netzwerksegmentierung können sich Mitarbeitende, die keinen Zugang benötigen, nicht mehr so frei im Netzwerk bewegen, wie es früher der Fall war, als alle im Büro waren. Aber das trifft auch auf diejenigen zu, die böse Absichten haben.

Wir müssen die Überwachung von Laptops und Systemen verbessern, damit schnell erkannt wird, ob sie gefährdet sind, und man wirksam reagieren kann. Dabei muss der gesamte Lebenszyklus unserer Technologien berücksichtigt und sichergestellt werden, dass jedes Gerät die neuesten Updates erhält. Genauso wichtig ist es, für Sicherheit am Ende des Lebenszyklus zu sorgen. Selbst wenn das Gerät das Gebäude verlässt, können sensible Daten immer noch gehackt werden, wenn sie nicht vorher sachgerecht entfernt werden.

Wir müssen stärker kontrollieren und besser verstehen, wer welche Daten sehen kann. Es gibt Lösungen, durch die man automatisierte Richtlinien für den Zugriff, die Bearbeitung und die gemeinsame Nutzung von Informationen festlegen kann. Dadurch behalten die Unternehmen die Kontrolle über kritische und sensible Daten und das Risiko eines absichtlichen oder versehentlichen Datenverlusts wird verringert.

...UND ÜBER BORD MIT DEM ALTEN!

Natürlich müssen wir auch an unsere Mitarbeitenden denken und daran, wie sie sich außerhalb der sicheren Umgebung des Büros verhalten. Heutzutage ist es gängige Praxis, sensible Geschäftsgespräche auch über Mobiltelefone zu führen. Meetings über Microsoft Teams und Zoom finden häufig in Cafés oder während der Zugfahrt statt. Sogar in Kneipen.

Durch die Zunahme des hybriden Arbeitens, findet die Beratung mit Kolleg:innen nicht mehr nur am Schreibtisch statt. Deshalb erleben wir auch feindliche Angriffe von Cyberkriminellen auf Kommunikationsplattformen wie WhatsApp und sozialen Plattformen wie LinkedIn. Wenn ein Mobiltelefon kompromittiert wurde, weil ein Phishing-Link geklickt oder ein Passwort oder eine PIN weitergegeben wurde, kann das gesamte Netzwerk gefährdet sein.

Wir müssen eine Sicherheitskultur aufbauen, in der alle Mitarbeitenden sensibel für potenzielle Risiken und deren Auswirkungen sind. Deshalb sollte man mit den Mitarbeitenden über das Thema Sicherheit so sprechen, dass sie damit konkret in ihrem persönlichen Leben etwas anfangen können. Wenn wir z. B. darüber sprechen, wie wichtig es ist, einen Passwortmanager und eine mehrstufige Authentifizierung für die Anmeldung bei persönlichen Konten zu verwenden, nicht auf Links in irgendwelchen E-Mails zu klicken und keine Informationen preiszugeben, dann dürfen wir hoffen, dass dieses gute Verhalten auch zum Vorbild im Berufsleben wird.

Es gibt keine Geheimtechnik, die sofort alle Datensicherheitsprobleme löst. Die Rückzahlung der Sicherheitsschulden im Hybridzeitalter bedeutet, alle Mitarbeitenden müssen umdenken und neue Ansätze umsetzen. Doch wirklich erfolgreich wird man nur sein, wenn die richtige Kombination aus Prozessen und Technologien für die Mitarbeitenden gefunden wird, um die Cybersicherheit und die Widerstandsfähigkeit eines Unternehmens zu verbessern. Tun Sie das Richtige und tun Sie es richtig – viel Glück!

Die NCC Group hat globale Experten für Cybersicherheit und Risikominimierung. Mehr als 14.000 Kund:innen weltweit vertrauen ihnen beim Schutz ihrer wichtigsten Vermögenswerte vor den sich ständig ändernden Bedrohungen. Durch Knowhow, Erfahrung und weltweite Präsenz ist das Unternehmen bestens aufgestellt, um Unternehmen bei der Bewertung, Entwicklung und Kontrolle ihrer Cyber-Resilienz zu unterstützen.

www.nccgroup.com

DIE WELT HAT SICH VERÄNDERT – UND MIT IHR AUCH DIE INFORMATIONS-SICHERHEIT

Erfolgreiches hybrides Arbeiten hängt in hohem Maße von Collaboration-Tools ab, mit deren Hilfe man über Netzwerke hinweg kommunizieren und Informationen austauschen kann. Diese Tools sind zwar für die hybride Belegschaft unverzichtbar, stellen aber auch kritische Schwachstellen dar, die von Cyberkriminellen gerne ausnutzen werden.

Und das haben sie in der Tat getan. Fernarbeitende waren in den ersten Tagen der Pandemie ein leichtes Ziel für Hacker, da sie häufig mit unbekannten Systemen arbeiteten und unwissentlich anfällig für Cyberangriffe waren. Gleichzeitig wurden in den Unternehmen die Ausgaben für Sicherheit als Teil der allgemeinen Budgetkürzungen heruntergefahren und so die Cyber-Resilienz verringert.[1] Das geschah vor dem Hintergrund einer langfristig verstärkten Konzentration auf den Datenschutz, lange bevor Covid-19 ein Begriff wurde.

Aufgrund der geänderten Datenschutzbestimmungen müssen Unternehmen stärker kontrollieren, wie Unternehmens- und personenbezogene Daten erfasst, verarbeitet und gespeichert werden. Dazu gehören auch die Daten, die sich auf Druckern und Multifunktionssystemen befinden. Wer sich nicht an diese Vorschriften hält, dem drohen nach der EU-DSGVO Geldstrafen von bis zu 4 % des weltweiten Jahresumsatzes oder 20 Millionen Euro (je nachdem, welcher Betrag höher ist).[2] Das britische Datenschutzgesetz von 2018 sieht gleichwertige steuerliche Sanktionen vor.

Doch ganz abgesehen von den finanziellen Risiken, durch Cybersecurity-Bedrohungen besteht auch die Gefahr von erheblichen Imageschäden. Dies ist für das Tagesgeschäft genauso schädlich – wenn nicht sogar noch schädlicher. Ein Beispiel: Das Softwareunternehmen SolarWinds war Anfang 2020 Ziel eines massiven Cybersecurity-Angriffs, der sich auch auf die Kund:innen des Unternehmens ausbreitete.[3] Dabei wurden große Unternehmen wie Microsoft und führende Regierungsbehörden angegriffen und es kam zur Offenlegung von sensiblen Daten. Das führte zu Geldstrafen in Höhe von 3 Millionen Dollar und hatte dauerhaft schädliche Auswirkungen auf den Ruf des Unternehmens.[4]

Das war damals, so ist es heute.

Arbeitsplätze haben sich seit Beginn der Pandemie so stark verändert, dass es noch schwieriger ist, mit den Bedrohungen Schritt zu halten. Bei der weiteren Entwicklung von Plänen für hybrides Arbeiten ist es umso wichtiger, dass auf eine dauerhafte Sicherheit geachtet wird.

[1] https://www.computerweekly.com/news/252484783/Coronavirus-Cyber-security-spend-to-slow-in-2020
[2] https://www.itgovernance.co.uk/dpa-and-gdpr-penalties
[3] https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12?r=US&IR=T
[4] https://www.jdsupra.com/legalnews/the-solarwinds-cyber-attack-the-6179862/

Von den Erfolgen bei der Informationssicherheit hört man im Allgemeinen nichts. Einige Unternehmen haben einfach Glück, andere sind wachsam – und es gibt bestimmte Verhaltensweisen, die diese Unternehmen eint. Dieses eBook befasst sich mit diesen spezifischen Verhaltensweisen und wie sie in Ihrem Unternehmen umgesetzt werden können. **Drei Schwerpunktbereiche stehen dabei am Anfang, die Führungskräfte und IT-Entscheider:innen als erstes berücksichtigen sollten.**

1 INFORMATIONSSICHERHEIT FÄNGT BEI IHREN MITARBEITENDEN AN

Cyber-Angriffe in den ersten Tagen der Pandemie nutzten häufig die Unkenntnis der Mitarbeitenden im Umgang mit neuen Kommunikationsplattformen – wie Videokonferenzen – und die allgemeine Unsicherheit dieser Zeit aus.[5]

Im Verizon Business Data Breach Investigations Report von 2020 wird hervorgehoben, dass die Cyber-Bedrohungen in allen Bereichen erheblich zugenommen haben. Dabei machen der Diebstahl von Zugangsdaten und soziale Angriffe wie Phishing und gefälschte Geschäfts-E-Mails mehr als 67 % aller Datenschutzverletzungen aus.[6] Dem Bericht zufolge ist bei 82 % aller Datenschutzverletzungen "das menschliche Element, einschließlich sozialer Angriffe, Fehler und Missbrauch" beteiligt. Auch wenn Ihre Belegschaft jetzt sicherer im Umgang mit Telearbeitstools und Ihr IT-Team besser vorbereitet ist, die Gefahr von Cyberangriffen und Datenschutzverletzungen ist nach wie vor sehr real.[7]

Hinzu kommt, dass die Mitarbeitenden selbst häufig nicht die sichersten Mittel zur Weitergabe von Informationen verwenden. „Schatten-IT“ ist das Stichwort. Darunter versteht man die Verwendung von IT-Systemen – Software, Geräte wie Drucker und Scanner, Apps und Dateispeicher –, die nicht vom Arbeitgeber bereitgestellt oder genehmigt wurden. Die Mitarbeitenden verwenden sie einfach, weil sie ihnen vertrauter oder einfacher zu bedienen sind. Das geschieht aus Bequemlichkeit und Effizienz und nicht in böser Absicht, doch es kann zu einem ernsten Problem werden.

Zum einen sind Systeme von der Stange weniger sicher als solche, die für den professionellen Einsatz entwickelt wurden. Zum anderen können die IT-Teams ihre Sicherheit nicht überwachen, wenn sie nicht von ihnen freigegeben wurden. Das öffnet Angreifern Tür und Tor. Nach unseren Untersuchungen aus dem Jahr 2022 muss immer noch jeder fünfte Mitarbeitende seine eigene Ausrüstung mitbringen. Und der gleiche Anteil hat Schwierigkeiten, IT-Support aus der Ferne zu erhalten.

Neben dem Bedarf an IT-Standardisierung und -Unterstützung ist auch folgender Punkt ganz entscheidend: Es dauert einfach seine Zeit, bis Menschen ihre Gewohnheiten ändern und neue Arbeitsweisen erlernen. 77 % der IT-Teams berichten, dass die Mitarbeitenden außerhalb des Unternehmens die vereinbarten Sicherheitsregeln nicht mehr befolgen.

Und wenn die Grenzen zwischen Arbeit und Privatleben verschwimmen, sinkt auch die Sensibilität für geschäftskritische Daten. Selbst Expert:innen werden nachlässig: In einer Umfrage unter IT-Sicherheitsmitarbeitenden in Nordamerika und Europa gaben 20 % der Teilnehmenden zu, dass sie während der Lockdowns Mitgliedern ihres Haushalts die Nutzung von Arbeitsgeräten gestattet haben.[8] Kinder, die Schularbeiten erledigen, oder Partner:innen, die auf YouTube surfen, scheinen harmlos. Doch es genügt ein Mausklick einer ungeschulten Person, um Hackern den Zugang zum Sicherheitsbereich eines Unternehmens zu ermöglichen.

77 % DER IT-TEAMS BERICHTEN, DASS DIE MITARBEITER AUSSERHALB DES UNTERNEHMENS DIE VEREINBARTEN SICHERHEITSREGELN NICHT MEHR BEFOLGEN.

Wenn Laptops, Telefone und gemeinsam genutzte Drucker in der Öffentlichkeit ohne angemessene Sicherheitsvorkehrungen genutzt werden – in Flughafen-Lounges, Bibliotheken, selbst in professionell geführten Co-Working-Spaces – besteht die zusätzliche Gefahr, dass Fremde die Gelegenheit zum Datendiebstahl nutzen. **Man weiß nie, wer einem gerade „über die Schulter schaut“**

Ebenso können Personen, die unterwegs arbeiten, die Datensicherheit gefährden, indem sie nicht ordnungsgemäß gesicherte Laptops oder Telefone mit einem öffentlichen Netz verbinden. Wenn diese Einfallstore entdeckt und für eine Cyber-Attacke genutzt werden, beeinträchtigt das nicht nur das reibungslose Tagesgeschäft eines Unternehmens, sondern kann auch schwerwiegende langfristige Folgen haben.

Selbst Unternehmen mit einer Belegschaft, die ausschließlich vor Ort arbeitet, sollten sich ihrer Stellung innerhalb der Lieferkette bewusst sein, denn andere kooperierende Unternehmen können möglicherweise Fernarbeit oder hybride Arbeitsformen eingeführt haben. Außerdem kann die Verlagerung in die Cloud dazu führen, dass konventionelle Sicherheits-Frameworks nicht mehr greifen. Doch die Sicherheit entwickelt sich so schnell wie die Kriminalität, und moderne Dienste wie Zero Trust sorgen für ständige Abwehrbereitschaft.

Die Gefahren können auch durch Aufklärung verringert werden. Als Unternehmen ist es wichtig, Sicherheits- und Compliance-Richtlinien aufzustellen und die Mitarbeitenden darin zu schulen, sie einzuhalten. Sicherheit darf niemals kurzfristig gedacht werden, sondern sollte zu den kontinuierlichen Unternehmens-Schwerpunkten auch im Hinblick auf Investitionen werden. Nur so wird das nötige Vertrauen erreicht, um Entscheidungen zu treffen und voranzukommen.

ZERO TRUST, EIN SICHERHEITSRAHMEN, DER EINE AUTHENTIFIZIERUNG, AUTORISIERUNG UND KONTINUIERLICHE ÜBERPRÜFUNG ALLER BENUTZER ERFORDERT, IST EIN KONZEPT, DAS SPEZIELL FÜR DIE HYBRIDE WELT ENTWICKELT WURDE.[9] HERKÖMMLICHE SICHERHEITSVERFAHREN ERFORDERN IN DER REGEL NUR EINE GÜLTIGE ANMELDE-ID UND EIN PASSWORT, UM ZUGANG ZU EINEM NETZWERK ZU ERHALTEN. BEI ZERO TRUST WERDEN MEHRERE PRÜFUNGEN DURCHGEFÜHRT, BEVOR EINER PERSON (ODER EINEM GERÄT) ZUGANG GEWÄHRT WIRD.

[5] *https://www.theguardian.com/technology/2020/may/24/hacking-attacks-on-home-workers-see-huge-rise-during-lockdown*
[6] *https://www.verizon.com/business/resources/reports/dbir/*
[7] *https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-april-2022-14-3-million-records-breached*
[8] *https://www.securitymagazine.com/articles/94997-it-security-professionals-demonstrate-excessive-trust-despite-concerns-with-remote-work-security-programs*
[9] *https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/*

2 INFORMATIONSSICHERHEIT SETZT SICH AUF DEN GERÄTEN FORT

Drucker, Scanner und andere Geräte aus dem Bereich des „Internets der Dinge“ können für Hacker, die wissen, wonach sie suchen müssen, offene Tore darstellen. Innerhalb eines sicheren Netzwerks, wie es normalerweise in Firmenbüros verwendet wird, bietet es die Möglichkeit, aus der Ferne auf Geräte zuzugreifen. Das hat zahlreiche Vorteile. Allerdings können manchmal, und meist ohne böse Absicht, Geräte mit ungesicherten Umgebungen und sogar direkt mit dem Internet ohne Passwörter oder Firewalls verbunden werden.[38]

Moderne Multifunktionsdrucker sind **Endgeräte** und ebenso leistungsfähig wie PCs. Das bedeutet, dass die Drucker-Firmware im Visier von Hackern ist, die versuchen, Zugriff auf das Netzwerk und die Unternehmensdaten zu erhalten. Ein Angreifer könnte beispielsweise E-Mail-Verzeichnisse ändern, um so Dokumente an Empfänger:innen außerhalb des Unternehmens zu senden. Oder über HTTPS übertragene Dokument könnten abgefangen und gelesen werden, wenn das Dokument und seine Daten nicht verschlüsselt sind.

WAS IST EIN ENDGERÄT?

UNTER ENDGERÄTEN VERSTEHT MAN ALLE SYSTEME, DIE EINE VERBINDUNG ZUM UNTERNEHMENSNETZWERK AUSSERHALB DER FIREWALL HERSTELLEN, Z. B. LAPTOPS, TABLETS, MOBILE GERÄTE, KASSENSYSTEME UND SELBSTVERSTÄNDLICH AUCH DIGITALDRUCKER.

„PRINTJACK“:
DER WATERGATE-SKANDAL DER DRUCKINDUSTRIE

Ende 2021 veröffentlichte ein italienisches Forscherteam einen Bericht, in dem zu lesen war, dass über 50.000 Drucker in Europa für virtuelle Angriffe aus der Ferne anfällig seien. Sie nannten drei Arten von Angriffen, sogenannte „Printjack attacks“.[11]

Bei der ersten handelt es sich um eine Art „Rekrutierungsprozess“: Eine Lücke im Netzwerk wird ausgenutzt, um Drucker mit kleinen Fehlern zu infizieren, so dass sie überlastet werden und mit der Zeit immer mehr Probleme bereiten. Die zweite ist schon ernster. Ein sogenannter „Papier-DoS-Angriff“ führt dazu, dass Aufträge wiederholt gedruckt werden, bis das Papier ausgeht, was zu erheblichen Störungen am Arbeitsplatz führt. Beim dritten und schwerwiegendsten Fall spricht man vom „Man-in-the-Middle-Einbruch“. Dabei greifen Hacker auf alle gedruckten Daten zu, während sie selbst unsichtbar bleiben.

Alle drei Arten von „Printjack“-Angriffen werden durch Schwachstellen in den Netzwerkverbindungen der Geräte möglich. Doch mit strengen Authentifizierungsmethoden und einem soliden Sicherheitskonzept lassen sie sich vermeiden.

Die Forscher stellten fest, dass die Vereinbarungen bezüglich DSGVO und ISO/IEC 27005: 2018 in ganz Europa sehr häufig nicht eingehalten wurden. Und von den 50.000 beanstandeten Druckern standen die meisten in Deutschland, Russland, Frankreich, den Niederlanden und Großbritannien.

Doch die Sicherheitsmaßnahmen sollten nicht nur die Geräte betreffen, die Ihre Teams aktiv nutzen. Haben Sie auch an die alten, verstaubten Laptops, Festplatten und Drucker gedacht, die in irgendeinem Lagerraum eingeschlossen sind? Was ist damit?

Daten, die auf Geräten am Arbeitsplatz gespeichert sind, werden oft übersehen. Aber die Sicherheitsrisiken enden nicht, wenn ein Gerät nicht mehr benutzt und weggeschlossen wird. „Aus den Augen aus dem Sinn“ ist hierbei keine Option. Wenn die Lebensdauer eines Gerätes ihr Ende erreicht, stellt alles andere als eine gründliche und professionell durchgeführte Datenlöschung eine echte Gefahr dar.

Stellen Sie sich einen Drucker vor, der schon seit Jahren in einem Lagerraum steht. Obwohl er nie wieder benutzt wurde, funktioniert er noch immer und ist weiter mit dem Internet verbunden. Solche unbeabsichtigten Hintertüren sind ein weiterer Zugang für versierte Hacker, vor allem, wenn sich die Mitarbeitenden ihrer Existenz bewusst sind.

Kurz gesagt, starke und robuste Sicherheit bedeutet, den gesamten Lebenszyklus der verwendeten Geräte im Blick zu haben, sie während ihrer gesamten Lebensdauer zu schützen, bis hin zur Entsorgung.

Und hybrides Arbeiten bringt ganz neue Herausforderungen mit sich, denn ein Teil der Geräteflotte steht bei den Mitarbeitenden zu Hause. Unsere Untersuchung zeigt, dass 73 % der Personen, die IT Entscheidungen treffen, nicht in der Lage sind, Daten von externen Druckern und Scannern sicher zu entsorgen. Deshalb ist es unerlässlich, einen umfassenden Überblick über den gesamten Lebenszyklus Ihrer Geräte zu haben.

Das fängt damit an, dass alles, was einen Stecker hat, aktiv überwacht und mit den neuesten Sicherheits-Patches aktualisiert wird. Bei der Entsorgung alter Geräte halten Sie sich an ein vorher festgelegtes Verfahren, das von der sicheren Löschung aller Daten über die Trennung der Geräte bis hin zur ordnungsgemäßen Vernichtung aller Festplatten reicht. Anschließend sollte detailliert überprüft werden, dass alle verbliebenen physischen Informationen von Geräten, USB-Steckplätzen, Medienfächern usw. entfernt wurden.

Man kann nicht vorsichtig genug sein. Das gilt nirgendwo mehr als bei der Datenentsorgung, bei der es nicht ausreicht, diese Schritte einfach nur zu befolgen. Ebenso wichtig ist es, genaue Aufzeichnungen zu führen, falls von offizieller Stelle einmal Belege gefordert werden.

[10] *Canon Research, 2022*
[11] *https://arxiv.org/abs/2111.10645*

3 KOMBINATION AUS BEWÄHRTEN VERFAHREN UND INTELLIGENTEN TECHNOLOGISCHEN RICHTLINIEN

Vor allem in der Einführungsphase eines hybriden Arbeitsmodells kommt es häufig vor, dass Mitarbeitende Geräte verwenden, die nicht vom Unternehmen bereitgestellt oder genehmigt wurden. Zudem ist es für IT-Teams schwieriger, sicherzustellen, dass diese Geräte richtig eingerichtet sind, die erforderlichen Updates erhalten oder sich deren Daten sicher verwalten lassen.

Die Mitarbeitenden zu schulen und für sie Leitlinien zu erlassen, ist zwar wichtig, aber wahrscheinlich nicht ausreichend, um alle Probleme der Informationssicherheit zu minimieren oder ganz zu vermeiden. Die Auswahl der geeigneten technologischen Prozesse und Protokolle kann dazu beitragen, Informationssicherheitsprobleme zu vermeiden, die durch menschliches Versagen verursacht werden.

WELCHE PHYSISCHEN EINSCHRÄNKUNGEN KÖNNTE IHR IT-TEAM ERLASSEN?

Multifunktionsdrucker verfügen über Hilfsmittel, die verhindern, dass unbefugte Personen auf Dokumente zugreifen. Dazu gehören PINs, ID-Karten und Berechtigungen auf der Grundlage von Funktion, Abteilung, Dienstgrad und mehr. Diese Instrumente bieten die Gewissheit, dass die vor Ort gespeicherten Informationen nicht in die falschen Hände geraten.

Eine weitere Möglichkeit ist eine Software zur Überwachung der E-Mails. Damit soll eine menschliche Schwäche umgangen werden: die Neugier beim Öffnen von E-Mails unbekannter Absender, und zwar ohne das Recht der Mitarbeitenden auf Privatsphäre zu verletzen. Das sollte auch in risikoreichen Zeiten wie diesen nicht auf der Strecke bleiben.

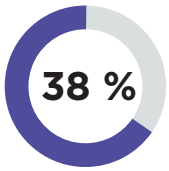
ABER WAS IST MIT DEN DATEN, DIE DAS BÜRO VERLASSEN?

Alle Unternehmen, die hybrid arbeiten, sollten Regeln für alle tragbaren Geräte aufstellen, die Informationen speichern, einschließlich Laptops, Diensttelefone und vor allem USB-Laufwerke. Es wird dringend empfohlen, Downloads und Installationen auf Firmenhardware ohne Genehmigung zu verbieten.

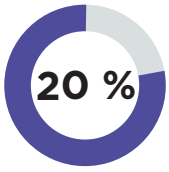
„MEHR ALS EIN VIERTEL (27 %) DER UNTERNEHMEN GABEN AN, DASS SIE VON BUDGETKÜRZUNGEN BETROFFEN WAREN, DIE SICH AUF IHRE AUSGABEN FÜR DIE CYBER-RESILIENZ IM JAHR 2020 AUSWIRKTEN.“[13]

[12] *https://www.youtube.com/watch?v=ZpGZEoYv8Ts*
[13] *NCC Group's Insight Space report, Paying off the cyber debt: How are decision makers approaching cyber resilience in 2021?*
[14] *https://www.securitymagazine.com/articles/94997-it-security-professionals-demonstrate-excessive-trust-despite-concerns-with-remote-work-security-programs*

In einer Umfrage unter IT-Sicherheitsexpert:innen in Nordamerika und Europa gaben 38 % der befragten Personen an, dass die Datenkontrolle während der Pandemie sehr schwierig zu handhaben war. Fast 20 % gaben an, dass ihre Arbeitsgeräte von anderen Haushaltsmitgliedern benutzt wurden.[14]



sagten, dass die Datenkontrolle während der Pandemie sehr schwierig zu handhaben war.



gaben an, dass ihre Arbeitsgeräte von anderen Haushaltsmitgliedern benutzt wurden

NCC GROUP WURDE OPFER EINES „MAN-IN-THE-MIDDLE-EINBRUCHS“, EINER NAHEZU UNSICHTBAREN ATTACKE.[12]

ATTACKE

Angreifer haben das Kundenportal von NCC attackiert. Indem sie den Datenverkehr des Portals auf ihr eigenes System umleiteten, hatten sie Zugriff auf die gesamte ein- und ausgehende Kundenkommunikation. Es handelte sich um erfahrene Hacker, das beweist die nahtlose Integration ihrer Infrastruktur in die Anmeldeseite des Portals.

HAUPTERKENNTNIS

Handeln Sie schnell und stellen Sie sicher, dass Ihre Risikobereitschaft mit der Sicherheit aller Drittanbietern des Unternehmens übereinstimmt. Veranlassen Sie außerdem geeignete Sicherheitsmaßnahmen in den Bereichen Prävention, Erkennung und Reaktion ein.

ANTWORT

Nachdem NCC festgestellt hatte, dass die Dateien kompromittiert worden waren, setzte man sich sofort mit den betroffenen Kund:innen in Verbindung. Anschließend wurden zur Schadensbegrenzung zwei Teams gebildet: ein technisches Untersuchungsteam und ein Krisenstab, der den Vorstand beriet.

„DA WIR SO SCHNELL REAGIERT HABEN, KONNTEN WIR DIE AUSWIRKUNGEN TATSÄCHLICH BEGRENZEN.“
– NCC GROUP

NEUE ARBEITSMODELLE, NEUE HERAUSFORDERUNGEN BEI DER SICHERHEIT

Bei der Planung künftiger Geschäftsmodelle sollten Sicherheit und Compliance stets im Mittelpunkt stehen. Ob Softwareplattformen, Hardware oder Governance – Ihr Unternehmen muss seine Sicherheitsstrategie kontinuierlich überprüfen, damit es auf die sich verändernde Bedrohungslage, die durch hybrides Arbeiten gefördert wird, vorbereitet ist.

Viele Unternehmen haben bereits Maßnahmen ergriffen: 48 % der an der europäischen Umfrage teilnehmenden IT-Führungskräfte möchten die Cybersicherheitsinfrastruktur in der Ära des hybriden Arbeitens bei Investitionen zu einem technologischen Schwerpunkt machen, und 40 % beabsichtigen, mehr für die IT-Schulung ihrer Mitarbeitenden auszugeben.[15] Falls Ihre Wettbewerber zu diesen Unternehmen gehören, sollten Sie nicht zögern: Kriminelle werden anfällige Unternehmen schnell ausgemacht haben.

Die digitale Transformation, die sich in vielen Unternehmen aufgrund der Pandemie beschleunigt hat, wird schon viele Sicherheits- und Compliance-Probleme beseitigt haben. Compliance mit der DSGVO kann beispielsweise bereits automatisiert und in Geschäftsprozesse integriert werden.

Aber es bleiben offene Fragen. Wo sind Sie sicherheitstechnisch verwundbar? Verfügen Sie über die Ressourcen, um die Probleme intern zu finden und zu beheben oder würden Sie externe Spezialisten einschalten, um ein ruhiges Gewissen zu haben? Sind sich alle Mitarbeitenden – von Neuangestellten bis hin zur Führungsebene – der Risiken bewusst, die mit dem hybriden Arbeiten verbunden sind? Würden Schulungen Ihnen das Vertrauen geben, kritische Geschäftsentscheidungen zu treffen? Und müssen Sie neue Richtlinien für die Nutzung von Bürohardware einführen, um die durch menschliches Verhalten verursachten Probleme zu entschärfen?

PROBLEME GELÖST: SICHERHEIT VERTEIDIGEN IN DER NEUEN ARBEITSWELT

Sich um das menschliche Verhalten zu kümmern, ist eine Sache, aber intelligente Technologien am Arbeitsplatz bieten Lösungen, die die Risiken auf das geringstmögliche Maß reduzieren.

IDC MarketScape bescheinigt Canon eine weltweit führende Rolle auf dem Feld der Sicherheitslösungen und -leistungen. Unsere Lösungen und Dienste tragen dazu bei, über den gesamten Informations-Lebenszyklus alle Dokumente und sensiblen Daten zu schützen (ob in Papier- oder digitaler Form), ohne dass die Arbeit der Menschen, die auf diese Informationen zugreifen müssen, dadurch beeinträchtigt würde. Das bedeutet, dass sie von Grund auf sicher sind, geprüft nach den höchsten Industriestandards und sich auf alle Aspekt der Informationssicherheit konzentrieren.

Dieser Sicherheitsansatz endet nicht mit dem Verkauf. Wir unterstützen Sie beim Schutz von Druck- und Scansystemen während ihrer gesamten Lebensdauer, von der Absicherung bis zur sicheren Entsorgung der Geräte, um sicherzustellen, dass die Daten jederzeit geschützt sind.

[15] *https://www.computerweekly.com/news/252500569/New-normal-of-remote-hybrid-working-sees-two-thirds-of-European-businesses-increase-IT-spend*

Der ganzheitliche Ansatz von Canon in Sachen Datensicherheit bedeutet, dass Informationen – egal, wo sie abgerufen, verwaltet und bearbeitet werden – leicht geschützt werden können.

DRUCKMANAGEMENT
Schützen Sie den Versand der druckfertigen Dokumente bis hin zur Druckausgabe am System. Indem Sie vernetzte Drucksysteme und alle druckbezogenen Nutzeraktivitäten absichern, verhindern Sie Datenmissbrauch.

ERFASSUNGSMANAGEMENT
Schützen Sie die Digitalisierung von Papierdokumenten und die Verteilung an den gewünschten Zielort. Indem Sie den Zugang zu Scanfunktionen kontrollieren und digitalisierte Dokumente schützen, erhöhen Sie die Dokumentensicherheit.

DOKUMENTEN- & CONTENT-MANAGEMENT
Schützen Sie die Speicherung und Bearbeitung von Dokumenten, ob auf Anwendungen vor Ort oder in der Cloud. Gewährleisten Sie die Einhaltung von Datenschutzbestimmungen und fördern Sie Maßnahmen zur Sicherheit von Dokumenten und Inhalten.

Unabhängig davon, wo Sie und andere Mitarbeitende arbeiten, unser Ansatz sorgt für Sicherheit – von der Cloud- oder Vor-Ort-Lösung bis hin zu Ihren Geräten. Durch Gespräche mit Kund:innen in der gesamten EMEA-Region haben wir vier gängige Arbeitsbereiche ausgemacht, die von Unternehmen in Kombination eingesetzt werden, um ihre neuen hybriden Arbeitsumgebungen zu gestalten.

Wir nennen sie hybride Hubs: Unternehmens-Hub (das konventionelle Büro in der Zentrale), Gemeinschafts-Hub (Co-Working-Bereiche und kleinere Satelliten-Büros), Homeoffice-Hub (Fernarbeit im Homeoffice) und Mobil-Hub (von unterwegs aus arbeiten – in Cafés, Bahnhöfen und Flughäfen oder während der Fahrt).

Es ist wichtig, die verschiedenen Standorte, die Ihre Mitarbeitenden nutzen, klar zu definieren und wie sie untereinander verbunden sind, da jeder Knotenpunkt seine eigenen Sicherheitsanforderungen hat. Wenn Sie diesen arbeitsplatzspezifischen Ansatz befolgen, können wir Ihnen helfen, einen durchgängigen Datenschutz zu gewährleisten.

Der Fokus von Canon liegt auf der Entwicklung des Arbeitsplatzes. Daher berücksichtigen wir bei jeder Kundenlösung alle Aspekte der Informationssicherheit. Letztendlich unterstützt die Digitalisierung wichtiger Geschäftsprozesse durch eine Reihe von Canon Lösungen nicht nur die Produktivität und Zusammenarbeit, sondern gibt der IT und den Abteilungen auch die Transparenz und Kontrolle, die sie benötigen, um gute Sicherheits- und Compliance-Praktiken in ihren Teams sicherzustellen.

Datenschutz ist wichtig – in einer hybriden Arbeitsumgebung mehr denn je –, sollte aber nicht verängstigen. Analysieren Sie Ihre Situation und ergreifen Sie Maßnahmen für eine erfolgreiche Zukunft.

Mehr Informationen finden Sie unter: www.canon.at/business/solutions

Kontakt
Canon Deutschland GmbH
Europark Fichtenhain A10
D-47807 Krefeld
Canon Helpdesk
Tel.: +49 69 299 936 80
canon.de

Canon Inc.
canon.com

Canon Europe
canon-europe.com
German edition

Canon Austria GmbH
Oberlaaer Straße 233
A-1100 Wien
Canon Helpdesk
Tel. +43 1 360 277 4567
canon.at

Canon (Suisse) SA
Richtistrasse 9
CH-8304 Wallisellen
Tel. +41 (0) 848 833 835
canon.ch