MEINUNGEN

CYBERSICHERHEIT: UND WENN MAN MITARBEITERN ZU IHREM EIGENEN WOHL GRENZEN SETZEN MÜSSTE?

Julien Paffumi
Product Management Leader, Stormshield

Homeoffice ist eine der offenkundigsten Auswirkungen der digitalen Transformation, wodurch sich die Möglichkeiten in den Unternehmen verändern, und eine der Reaktionen auf die derzeitige Gesundheitskrise. Abhängig von den Gewohnheiten und Verhaltensweisen der Mitarbeiter können diese neuen Verwendungszwecke dazu führen, die Sicherheit der Unternehmen zu untergraben. Sollten daher der Zugang und die Funktionalitäten bestimmter Desktop-Arbeitsplätze eingeschränkt werden, um die Sicherheit des gesamten Unternehmens zu gewährleisten? Wenn man wieder zu einer Zeit zurückkehrt, in der es notwendig war, Zugriffs- und Installationsrechte für einen PC-Arbeitsplatz zu beantragen, könnte das zusätzliche Schutzschilder bieten, IT-Abteilungen jedoch in eine Zwickmühle bringen.

Mit der digitalen Transformation, der Virtualisierung von Dienstleistungen und der Mobilität von Arbeitnehmern verschieben sich die Grenzen des Unternehmens, und die Bereiche zwischen Arbeit und Privatleben verschwimmen immer mehr. Ob der Zugriff auf das interne Netzwerk über ein ungesichertes WLAN oder das Kopieren und Einfügen eines wichtigen Unternehmensdokuments über einen persönlichen USB-Stick erfolgt - es wird eine immer größere Anzahl von verschiedenen Geräten verwendet und untereinander verbunden. Eine Klarstellung gleich zu Beginn: Diese Tatsache beschränkt sich auf keine Hierarchie; der ahnungslose Auszubildende, der gestresste kaufmännische Angestellte oder der CEO, der sich für unverwundbar hält: Sie alle sind potenzielle Überträger von Cyberrisiken. Zumal viele von ihnen Administratorenzugriff auf ihren Desktop-Arbeitsplätzen haben. Es stellt sich die Frage: **Sollen wir zu „früheren" Praktiken zurückkehren und allen zu ihrer eigenen Sicherheit Beschränkungen auferlegen?**

Eine Frage, die in der aktuellen Gesundheitskrise vielleicht noch relevanter wird, da Notfallsituationen und Cybersicherheit nie vereinbar sind. Um es Unternehmen zu ermöglichen, ihre Aktivitäten aufrechtzuerhalten, halten digitale Dienste, insbesondere Homeoffice, in den Wohnungen der Mitarbeiter Einzug. Aber mit ihnen werden auch die Schwachstellen im Unternehmen an die Mitarbeiter weitergeleitet. „*Mit der Covid-19-Pandemie werden Unternehmen, die nicht wegen der Wirtschaftskrise zugrunde gehen, infolge von Computerangriffen zunichte gemacht*", prophezeit der CISO eines großen Unternehmens im Bereich Luftfahrt. Diese Aussage fasst in wenigen Worten die Ängste einer ganzen Branche in einer Zeit zusammen, in der sich eine seit einem Jahrhundert beispiellose Gesundheitskrise auf die ganze Welt ausbreitet.

„Mit der Covid-19-Pandemie werden Unternehmen, die nicht wegen der Wirtschaftskrise zugrunde gehen, infolge von Cyberangriffen zunichte gemacht".

***Ein CISO** eines großen Unternehmens der Luftfahrtbranche*

Wagen wir es also, eine Parallele zwischen dieser beispiellosen Gesundheitskrise und den Beschränkungen für Mitarbeiter zu ziehen. Die Entscheidung der Regierung, die Bevölkerung zu Hause zu isolieren, ist eine restriktive Maßnahme, aber entspringt der Notwendigkeit, die Sicherheit der Gemeinschaft zu gewährleisten. Es stellt sich die Frage, ob wir uns in Bezug auf Cybersicherheit ein Beispiel daran nehmen sollten?

AUTONOMIE UND EFFIZIENZ, EIN UMFELD VON BESCHRÄNKUNGEN

Eine mögliche Antwort liegt darin, Arbeitnehmer haftbar zu machen, was in einigen Fällen zu Sanktionen führen kann. Aber ist diese Lösung wünschenswert? Eine andere Möglichkeit wäre, zur Beantragung von Zugriffs- und Installationsrechten auf einen PC-Arbeitsplatz zurückzukehren, wie das früher üblich war. Ist dies in der heutigen Geschäftswelt praktikabel, in der viele Mitarbeiter direkt für ihre PC-Arbeitsplätze Administratorzugang haben? „*Um zu verstehen, wie es in einigen Unternehmen zu*

dieser Entwicklung gekommen ist, müssen zwei Szenarien berücksichtigt werden. Auf der einen Seite hegen bestimmte Mitarbeiter, die über fortgeschrittene IT-Kenntnisse verfügen und selbst bestimmte Anwendungen installieren, Skripte schreiben oder Vorlagen erstellen wollen, ohne die IT-Abteilung jedes Mal um diese oder jene Genehmigung bitten zu müssen, den Wunsch nach Selbständigkeit", erläutert **Franck Nielacny**, CIO bei Stormshield. „*Es gibt noch einen zweiten Faktor zu berücksichtigen, der sich auf die Verfügbarkeit und Reaktionsfähigkeit der IT-Teams bezieht. In bestimmten Kontexten muss ein CIO auf viele Anfragen reagieren und diese nach Prioritäten verwalten. Manchmal ist es also am einfachsten, Zugang zu den Admin-Rechten zu ermöglichen.*"

Es wird jedoch empfohlen, einige einfache Regeln bezüglich Filterung und Zugangsbeschränkung zu befolgen. „*Meine Empfehlung umfasst zwei Dinge: Funktionen, die keinen ausgeprägten technischen Schwerpunkt haben, benötigen kein Administratorkonto. Für technischere Bereiche wäre der Idealfall, zwei Konten einzurichten, ein allgemein verwendetes Standardkonto und ein Administratorkonto. Letzteres sollte dabei so eingeschränkte Funktionalitäten wie möglich haben und einen fest umgrenzten Rahmen von Anwendungen beinhalten, die in einer IT-Charta festgelegt sind*", erklärt Franck Nielacny.

BESCHRÄNKEN,BLOCKIEREN, VERANTWORTLICH MACHEN:EIN CYBERWALZER IN DREI TAKTEN

In einem normalen Kontext ist es schwierig, sich einen Ansatz vorzustellen, bei dem Mitarbeiter einer vollständigen Beschränkung unterliegen. Wie kann man die Reaktion der Arbeitnehmer auf Maßnahmen abschätzen, die sie als zu restriktiv oder als Verletzung ihrer Grundrechte ansehen? „*Nur in einem äußerst kritischen Kontext, in dem das Unternehmen wirklich in Gefahr ist, wäre es gerechtfertigt, für alle Mitarbeiter auf strenge Beschränkungsmaßnahmen zurückzugreifen*", so Franck Nielacny weiter. *Diese dürfen allerdings nur vorübergehend sein.*" Die gegenwärtige Situation, die durch eine doppelte Einschränkung von Autonomie und Effizienz gekennzeichnet ist, scheint ihm in diesem Moment recht zu geben: Weil die Situation außergewöhnlich und vorübergehend ist, werden diese Beschränkungen akzeptiert.

Ein weiteres Beispiel für Beschränkungen: Abzuschätzen, ob der Zugang zu persönlichen E-Mails oder Nachrichten im beruflichen Kontext erlaubt werden soll oder nicht. Auch hier wäre der Mittelweg, den Zugriff zu erlauben, aber das Anklicken von Anhängen zu verbieten und auf diese Weise das Bewusstsein für das Infektionsrisiko von Computern zu erhöhen. Denn, vergessen wir nicht, die Gefahr der Umgehung und damit der Schatten-IT ist allgegenwärtig! „*Es ist wichtig, realistisch zu sein*", betont Franck Nielacny. „*Wir alle leben heutzutage in einem Arbeitsumfeld in dem Berufs- und Privatleben nah beieinander liegen. Mit dem Covid-19 und der häuslichen Isolation wird Schatten-IT für alle Unternehmen noch mehr zur Realität. Die Herausforderung besteht darin, eine maximale Undurchlässigkeit mit dem IT-System des Unternehmens zu gewährleisten,*

indem der Datentransfer mit Drittsystemen eingeschränkt wird." *Sensibilisierung und Verantwortungsbewusst sind daher schon im Vorfeld unerlässlich.* Wir können nie oft genug darauf hinweisen, wie nützlich die Einführung einer Kultur für effiziente Cybersicherheit ist.

ALLGEMEINER RÜCKGANG DES SICHERHEITSNIVEAUS ANGESICHTS COVID-19

In Frankreich gibt das Innenministerium am 16. März 2020 in einer Situation, in der die übereilte Umorganisation der Arbeitsumgebungen in Richtung Homeoffice enorme Risiken für die Unternehmen mit sich bringt, eine Mitteilung heraus, in der darauf hingewiesen wird, dass „*ein verstärktes Auftreten von Cyber-Angriffen wie „Datendiebstahl" bzw. Erpressungssoftware (Ransomware) für Unternehmensnetzwerke absehbar ist, die versuchen, die mögliche Verringerung der Aufmerksamkeit oder die fehlende Organisation auszunutzen.*" „*Bei Ausbruch der Covid-19-Pandemie waren die Unternehmen nicht darauf vorbereitet. Die meisten reagierten überhastet*", bestätigt der CISO eines großen Unternehmens im Luftfahrtsektor. „D*ie Krise findet in einem Kontext statt, in dem IT-Abteilungen keine Entscheidungsbefugnis haben und ihre Budgets weitgehend unzureichend sind.*" Schlechte Vorbereitung, Einfrieren der IT-Budgets … die Gesundheitskrise könnte für einige Unternehmen unvorhersehbare Folgen haben. Dies gilt umso mehr, als es in diesem Zusammenhang – um die wirtschaftliche Folgen vorwegzunehmen – vorrangiger ist, die Geschäftskontinuität und -fortführung vor Fragen des IT-Sicherheitsmanagements zu stellen. Allen ist klar, dass die Lage ernst ist. Im Fall von strategisch wichtigen Einrichtungen an vorderster Front, wie z. B. Krankenhäuser, besteht die Herausforderung darin, „*ergonomische und wirksame Lösungen*" umzusetzen, wie **Cédric Cartau**, CISO des Universitätskrankenhauses von Nantes, in seinem Beitrag „*La DSI face au COVID*" (dt. Die Leitung der IT-Systeme angesichts von COVID) (auf DSIH. fr) erklärt.

Zusätzlich zu Beschränkungen ist es auch notwendig, die möglichen und risikoreichsten Übertragungswege für Cyberrangriffe zu kontrollieren. Bestimmte Technologien können so ein anormales Verhalten einer Maschine, die versucht, eine Schwachstelle auszunutzen, einen plötzlichen Anstieg der Anzahl der Anfragen, geografisch unmögliche Benutzerverbindungen (z. B. in Australien am späten Vormittag und in New York am frühen Nachmittag) oder die Verwendung ungewöhnlicher Befehle erkennen. Es liegt dann am CISO, die „Norm" für unverdächtiges Verhalten, die Baseline, richtig festzulegen, um die Sicherheit zu erhöhen, ohne dem Benutzer Beschränkungen auferlegen zu müssen.

ZERO-TRUST, EIN PARADIGMA FÜR DIE ZUKUNFT?

Wie wir gesehen haben, machen Krisensituationen die Neuauslegung der Unternehmensgrenzen und die zunehmende Mobilität der Mitarbeiter ein Umdenken bei der Sicherheit von Informationssystemen notwendig. In diesem Zusammenhang ist immer öfter vom Zero-Trust-Ansatz die Rede. Die Herausforderung? Die Anwendung eines echten Zero-Trust-Ansatzes bei Benutzern, Terminals oder PC-Arbeitsplätzen und die maximale Kontrolle des Austausches zwischen einer Maschine und dem Rest ihrer Umgebung. „*Dank diesem Modell kann das Unternehmen kontrollieren, wer worauf, wie und wann Zugriff hat*“, sagte **Pierre-Yves Popihn**, technischer Direktor bei der NTT Security France in Les Echos.

Zusammenfassend lässt sich sagen, dass es neben dem Schutz vor erwiesenen Bedrohungen und anormalem Verhalten daher unerlässlich ist, bestimmte Sperren auf Arbeitsplatzebene einzurichten. Dies muss jedoch in einem Ansatz geschehen, der auch Raum für das Bewusstsein für digitale Hygiene und die Verantwortung der Benutzer lässt. Eine der Lehren aus der gegenwärtigen Gesundheitskrise ist, dass - was immer man auch denken mag - diese Regeln und Selbstdisziplin notwendig sind, um eine anhaltende Bedrohung einzudämmen. Angesichts eines sich verändernden Kontextes muss auch anerkannt werden, dass sich der Grad der „*Strenge*“ dieser Regeln ändern kann und muss. Anpassung ist daher hier die Lösung. Um dies zu erreichen, ist es entscheidend, Verbindungen zum persönlichen Leben der Beschäftigten zu schaffen. „*Wenn die Menschen davon überzeugt sind, dass dies Auswirkungen auf ihr Privatleben haben kann, werden sie es auch in ihrem Berufsleben berücksichtigen*“, betont unser Kollege aus dem Luftfahrtsektor.

STORMSHIELD

Weltweit müssen Unternehmen, Regierungsinstitutionen und Verteidigungsbehörden die Cybersicherheit ihrer kritischen Infrastrukturen, sensiblen Daten und Betriebsumgebungen gewährleisten. Die auf höchster europäischer Ebene zertifizierten Stormshield-Technologien sind die richtige Antwort auf IT- und OT-Risiken und erlauben den Schutz der Geschäftstätigkeit. Unsere Mission: Cybersorglosigkeit für unsere Kunden, damit diese sich auf ihre Kerntätigkeiten konzentrieren können, die für das reibungslose Funktionieren von Institutionen, Wirtschaft und Dienstleistungen für die Bevölkerung so wichtig sind. Die Entscheidung für Stormshield ist eine Entscheidung für eine vertrauenswürdige Cybersicherheit in Europa. Weitere Informationen finden Sie unter www.stormshield.com.