Stufen von Cybersicherheit – frei nach Hermann Hesse

16 April 2020 | **Cyber Security** | **Lena Csomor, Raphael Reischuk**
Lesezeit: 7 Minutes

In Zeiten von COVID-19 geraten Bedrohungen aus dem Cyberspace etwas aus dem Fokus der Öffentlichkeit. Doch gerade in Zeiten von verstärktem Remote Working sind Cyberangriffe so gefährlich wie nie zuvor. Eine zeitgemässe Anlehnung an das Gedicht «Stufen» von Hermann Hesse.

Zwischen all den von Angst und Unsicherheit geprägten Nachrichten, die zurzeit allgegenwärtig sind, gibt es noch Zeichen von Produktivität und Fortschritt. Die Mittel dazu gibt uns die Digitalisierung, die nun zwangsläufig in jeden Winkel des (Arbeits-)Lebens vordringt. Sie hält die Bildungsanstalten, Banken und Büros aller Art am Laufen. Manch einer hat sich an die neue Situation gewöhnen können, die einen in Jogginghosen, die anderen im Sakko vor der Kamera. Einzig eine Gruppe kann ihnen in punkto Anpassungsfähigkeit den Meister zeigen: Hacker und Cyberkriminelle.

Cyberangriffe sind besonders in Zeiten von Home Office und Remote Desktop eine bedeutende, wenn auch meist unsichtbare Gefahr, die genauso wenig vor der Haustüre Halt macht wie das pandemische Virus. Angst ist hier jedoch kaum angebracht. Es gibt einfache Wege, sich und Mitarbeitende mit messbarer Effektivität zu schützen. Während bisher oft ausschliesslich die IT-Spezialisten für Cybersicherheit verantwortlich waren, zwingt das Home Office nun auch vermehrt unerfahrene Nutzer, sich mit der Thematik der Cybersicherheit auseinanderzusetzen. Wie vorteilhaft und wichtig ist diese Entwicklung? Und welchen technischen Herausforderungen muss sich die Gesellschaft während und nach der Krise stellen?

Sich in Tapferkeit und ohne Trauern in andre, neue Softwareintegration zu geben

Die Überlastung der gewohnten Infrastruktur (beispielsweise unternehmensweite VPNs oder etablierte Kollaborationstools) zwingt IT-Departemente dazu, rasch neue Wege zu finden, um die Erreichbarkeit von Services und Mitarbeitenden zu garantieren. Dies führt möglicherweise zur unstrukturierten Integration neuer Software, mit der IT und Mitarbeitende selbst nur wenig vertraut sind und deren Kompatibilität und Sicherheitsqualitäten nur ungenügend überprüft wurde. Selbst wenn die Lösung oberflächlich scheinbar funktioniert, besteht die Gefahr, dass solche «Dirty Hacks» in der Systemlandschaft bestehen bleiben.

Erschwerend kommt hinzu, dass viele Anwendungen im Moment grossen Stresstests

unterzogen werden. Das führt positiverweise dazu, dass Software-Entwickler gezwungen sind, grundsätzlich stabilere Anwendungen zu bauen. Gleichzeitig werden auch mehr Bugs und Sicherheitslücken ans Licht kommen, was längerfristig ein Gewinn für die Nutzer von Anwendungen sein wird, weil die Schwachstellen häufiger und schneller gepatcht werden. Kurzfristig sind die Nutzer aber eher mehr Hackern ausgeliefert, da viele Hersteller überlastet sind oder aktuell nicht genügend Budget und Ressourcen zur Verfügung haben.

Trotzdem geniesst die IT-Sicherheit nicht die höchste Priorität vieler Unternehmen, da vor allem möglichst schnell und möglichst viele Geräte für ihre Mitarbeitenden aufgesetzt werden müssen. Derartig überhastete Prozesse schaffen oft unbemerkt Sicherheitslücken, die es Hackern erlauben, die Systemlandschaft zu infiltrieren. Bleiben die Eindringlinge unbemerkt, sind sie wahrscheinlich auch nach der Pandemie noch auf den Systemen und nutzen Gelegenheiten, wo sie sich bieten.

Solche Szenarien stellen grosse Anforderungen an fast alle Unternehmen. Doch es braucht nicht Resignation, sondern Bewusstsein für die Situation. Alle Änderungen an der Systemlandschaft müssen unbedingt sauber protokolliert werden, auch wenn im Moment keine Sicherheitsprüfungen stattfinden. Es sollten alle neuen und kurzfristig modifizierten Geräte möglichst so behandelt werden, als wären sie mit Malware infiziert, ohne es zu merken – entsprechend sollte eine Sicherheitsprüfung der Geräte stattfinden, sobald die Sicherheitsanforderungen wieder erfüllt werden können.

Mit systematischen Aufzeichnungen dieser Probleme kann eine Art «Technical Security Debt» erstellt, nachvollzogen und möglichst zeitnah wieder getilgt werden. So ist sichergestellt, dass nach dem ersten Chaos schnell wieder Ordnung herrschen kann. Besser noch, es kann eine resilientere, sicherere IT-Infrastruktur daraus hervorgehen, die an die Bedürfnisse der Mitarbeiter hervorragend angepasst ist.

Und jedem Anfang wohnt ein Zauber inne, der uns aber nicht alleine beschützen kann

Plötzlich alleine gelassen im Home-Office wünscht sich mancher die Nähe des IT-Supports zurück. Wieder ist die Anpassungsfähigkeit der Mitarbeitenden gefragt, die sich nun selbst helfen und eine höhere Kompetenz im alltäglichen Umgang mit Technik entwickeln müssen. Dieser Prozess mag beschwerlich sein, ist aber in vielen Unternehmen längst überfällig und nötig. Langfristig werden alle Beteiligten von diesen neuen Fähigkeiten profitieren, durch gesteigerte Effizienz und weniger Ärger.

Man muss sich jedoch bewusst sein, dass ungeachtet der initialen Kompetenz nun alles und jeder aufs ungefilterte Internet losgelassen wird – das birgt grosse Risiken, denn die meisten

Lernprozesse finden nun über das Arbeitsgerät statt. Es ist darum im Sinne der Arbeitgeber, ihren Mitarbeitenden möglichst rasch gewisse Grundkenntnisse (nicht zuletzt im Bereich der IT-Sicherheit) verständlich und einfach zu vermitteln. Die Fähigkeit zur Risikoeinschätzung und -erkennung sollte dabei im Vordergrund stehen.

Auch die Arbeitsgeräte selbst stellen Unternehmen vor neue Herausforderungen – denn wann ist ein Arbeitsgerät als ein solches definiert? Im einfachsten (und sichersten) Fall haben die Mitarbeitenden ihr vertrautes Gerät aus dem Büro nach Hause genommen; es verfügt also zumindest lokal über die Sicherheitsstandards, die zuvor vom Unternehmen etabliert wurden. Gerade im Home Office, wo die Grenzen von Privatem und Arbeit oft verschwimmen, sind «ortsfremde» Arbeitsgeräte besonders gefährdet. Es muss davon ausgegangen werden, dass sich die Nutzer weniger diszipliniert verhalten und unsichere Software downloaden oder gefährliche Links klicken, wider besseres Wissen – denn zu Hause fühlen Menschen sich vertraut und folglich sicher, auch vor Cyberattacken.

Noch gefährlicher wird es, wenn wenig gesicherte private Geräte plötzlich als Arbeitsgeräte herhalten müssen. Geschäftsdaten werden dann auf nicht vertrauenswürdige Geräte geladen und bleiben eventuell bis lange nach der Pandemie dort, wenn der Nutzer vergisst, sie zu löschen. Deshalb sollte spätestens, wenn die Mitarbeiter ins Büro zurückkommen darauf hingewiesen werden, dass sie auch ihre privaten Geräte «aufräumen» müssen.

Die Liste der Probleme ist lang, und der Umgang mit sensiblen Daten steht bei einigen Unternehmen weit oben; sie mussten einen Teil ihrer Abläufe in sehr kurzer Zeit papierfrei organisieren. Dokumente und andere Daten werden jetzt vollständig via E-Mail verschickt; das Fax hat endlich ausgedient. Man kann davon ausgehen, dass viele Mitarbeitende ungenügend informiert wurden, wie sie sensible Daten via E-Mail verarbeiten müssen, da diese zuvor nur auf Papier und in geschützten Datenbanken vorhanden waren. Dadurch, dass jetzt jeder im eigenen, vom Arbeitgeber unkontrollierten Netzwerk arbeitet, bietet sich eine wesentlich grössere Angriffsfläche als vor Ausbruch der Pandemie. Ein einziges infiziertes Home-Netzwerk kann bereits ausreichen, um wertvolle Daten und vertrauliche Kommunikation abzugreifen. Werden diese Daten jetzt gestohlen, kann das langfristige Folgen für die Unternehmen und entsprechend für ihre Kunden haben.

Eine mögliche Lösung für private Geräte als Arbeitsgeräte bietet der Virtual Desktop. Er behebt als technische Lösung zwar nicht das Problem der oft fehlenden Awareness, kann aber eine technisch sicherere Umgebung bieten und gibt dem Unternehmen wieder etwas Kontrolle zurück.

Des Lebens Ruf an uns wird niemals enden

Mangels anderweitiger Beschäftigung und dank Eltern am Laptop lernen auch Kinder längst überfällige IT-Skills wie beispielsweise das Programmieren. Fotos von Kindern, die es «den Grossen» gleichtun wollen und neben den Eltern am Computer sitzen, erscheinen zu Hauf – viele Eltern (besonders die technikaffinen) ermutigen den Nachwuchs dann gleich, das Gerät und seine Funktionalitäten besser kennenzulernen. Homeschooling fördert das Bedürfnis, dass die Kinder eigenständig mit Computern und Tablets klarkommen. Das tun sie auch, oft in beängstigender Geschwindigkeit!

Sicherheitsprobleme wird es immer geben. Für das Home Office sind die Kinder von heute auf jeden Fall vorbereitet – solange wir, die Grossen, mit gutem Beispiel vorangehen. Erzwungene Zeit im Home Office bietet eine Fülle an Möglichkeiten. Es ist von enormer Wichtigkeit, dass Sicherheit dabei eine hohe Priorität erfährt und nicht aus Zeitgründen immer wieder beiseitegeschoben wird. Nehmen wir uns die nötige Zeit und machen die Welt sicherer und hoffentlich dann auch gesünder.

Überschriften frei angepasst nach dem wunderschönen Gedicht «Stufen» von Hermann Hesse, welches uns in jeder Krise Mut fassen lässt.