Rechner und Netzwerke überprüfen

„Cyberhygiene“ nennt man Schutzvorkehrungen, mit denen man Computer und Netzwerke „sauber hält“ und Schaden abwendet, den elektronische Eindringlinge und Angriffe verursachen können.

Körperhygiene trägt zum persönlichen Wohlbefinden bei, hygienische Produktionsbedingungen führen zu hoher Lebensmittelsicherheit, jeder möchte gerne in Restaurants essen oder in Hotels absteigen, in denen er hygienische Bedingungen vorfindet. Der aus dem Griechischen stammende Begriff „Hygiene“ bezeichnet eine der Gesundheit zuträgliche Kunst und Wissenschaft. In den letzten Jahrzehnten ist das Internet in der Mitte unserer Gesellschaft angekommen. Computer und Netzwerke werden nicht mehr nur als Hilfsmittel zur Datenverarbeitung verwendet, sondern begleiten unser ganzes Leben. Daher ist es wichtig, dass wir neben dem Funktionieren der materiellen Welt auch die Unversehrtheit der elektronischen Welt sicherstellen.

„Cyberhygiene“ ist ein Sammelbegriff für Schutzvorkehrungen, mit denen man Computer und Netzwerke „sauber hält“ und damit Schaden abwendet, den elektronische Eindringlinge und Angriffe verursachen können. In Anlehnung an Hygienekonzepte im Gesundheitsbereich geht es um drei Themenkreise:

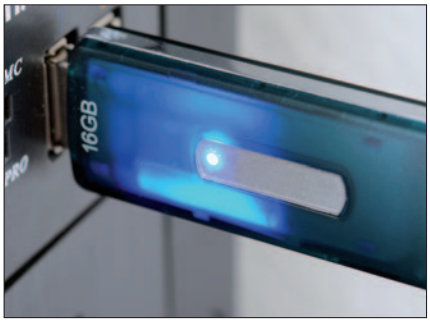
1. Welche Hilfswerkzeuge und Prozeduren stehen zur Verfügung?

Als Analogie zu Desinfektionsverfahren stehen im elektronischen Bereich Programme zur Verfügung (wie Firewalls, Schadsoftwarescanner), die kombiniert mit den richtigen Verfahren (beispielsweise Mehr-Faktor-Authentifizierung, Verschlüsselung) Schädlinge abwehren.

2. Wie kann man Sicherheitsmaßnahmen in die Routine des Arbeitsalltags integrieren?

Die Betreiber von Computern und Netzwerken – seien das Einzelpersonen, Firmen oder Organisationen – müssen Strategien entwickeln, dass ohne Zutun der Benutzer automatisch bestimmte Verfahren ablaufen – zum Beispiel die periodische Datensicherung, das Update von Softwarekomponenten, das Auswerten von Zugriffsprotokollen von Computern und Firewalls oder das Prüfen von Datenabflüssen.

Mitarbeiter sollten über Cyber-Sicherheitsmaßnahmen informiert werden.



Vorsicht: USB-Sticks könnten mit Schadsoftware verseucht sein.

3. Wie kann man die Effizienz der Werkzeuge sicherstellen?

Wie bei vorgeschriebenen Hygiene-Prozeduren in Gesundheitseinrichtungen ist es notwendig, dass die Anwender laufend mit der Cyberhygiene konfrontiert werden, indem sie beispielsweise ihr Passwort ändern müssen, ihren Fingerabdruck eingeben müssen, oder bestimmte Daten nach einer gewissen Zeit unwiderruflich gelöscht werden.

Aufklärung und Kehraus. Damit all diese Schutzwerkzeuge und Abläufe greifen, ist es notwendig, grundsätzliche Fragen zu klären und einen „Frühjahrsputz“ durchzuführen. Zuallererst betrifft das die Datenhygiene: Welche Daten befinden sich in welchen Systemen und wie sind sie geschützt? Welche Daten werden wirklich benötigt, wer hat darauf Zugriff und wie können nicht benötigte oder alte Daten sicher gelöscht werden?

Ähnliches gilt für Programme: Was ist installiert und was wirklich davon in Verwendung – und welche internen oder externen Benutzer haben die Rechte, diese Programme auszuführen?

Das Deinstallieren oder Deaktivieren unbenutzter Programme oder Services führt zu verbesserter Ablaufgeschwindigkeit und Speichernutzung. Der Widerruf von Benutzerrechten gehört regelmäßig nach dem Prinzip durchgeführt, dass die Anwender nur die notwendigen Zugriffsrechte haben sollten.

Überdies muss die stationäre und mobile Hardware elektronisch erfasst und beobachtet werden. Dazu gehören Geräte, die nicht als Computer erkennbar sind, weil sie am „Internet der Dinge“ hängen (z. B. Kameras, Türöffner, Netzwerkkomponenten). Alte Hardware muss ausgetauscht oder auf den neuesten Stand gebracht werden, und unsichere Geräte müssen überhaupt vom Netz.

Die Mitarbeiterinnen und Mitarbeiter sollten in Aufklärungs- und Fortbildungsmaßnahmen über Angriffsmethoden informiert werden, die über soziale Wege vorgenommen werden (z. B. Phishing-E-Mails, CEO-Betrug). Einmal im Jahr sollten solche Angriffe simuliert werden, damit klar ist, ob die Organisation die Risiken ernst nimmt.

Vorbeugung und Quarantäne. Kommt es zu Angriffen, deren Gründe oder Ausmaß unklar sind, oder zu Befall mit Schadsoftware, sollten die betroffenen Systeme vom Netz genommen werden, bis sie gründlich untersucht werden konnten. Dies ähnelt den Quarantäne-Stationen im Gesundheitsbereich, in denen Patienten mit resistenten Keimen oder mit gefährlichen Infektionen isoliert untergebracht werden, um andere nicht zu gefährden.

Damit es nicht soweit kommt, müssen die Einfallstore geschlossen werden. Besondere Vorsicht gilt bei der Verwendung von Memory-Sticks, da diese mit Schadsoftware verseucht sein können, die einen Computervirenbefall oder die Installation eines geheimen Kanals zu virtuellen Angreifern ermög-

FOTO: DJAMA/STOCK.ADOBE.COM, MANGOSTAR/STOCK.ADOBE.COM

Cyberhygiene-Check-up“: Einmal im Jahr sollten Computersicherheit und Datenintegrität untersucht werden.

licht. Aber auch die Verwendung von USB-Anschlüssen, um mobile Geräte an einem fremden Computer aufzuladen, birgt Risiken, da sich beispielsweise bei einem entsperrten Android-Smartphone je nach Sicherheitseinstellung nahezu alles auslesen lässt. Bei Apple-Produkten werden in neueren Betriebssystemversionen automatisch alle Datenzugriffe blockiert, wenn die Gerätesperre mehr als eine Stunde aktiv ist.

USB-Kondome. Ein möglicher Angriff über Schwachstellen im System ist aber nie völlig auszuschließen, wenn eine Datenverbindung zum Gerät besteht. Daher ist eine reine Stromverbindung sicherer. Diese kann durch die Verwendung von „USB-Kondomen“ erreicht werden. Ein solches Kondom besteht aus einer USB-Buchse auf der einen und einem Stecker auf der anderen Seite. Steckt man es zwischen Ladekabel und Buchse, leitet es nur den Strom weiter und blockiert dabei die Datenleitung. Für diese Zwecke gibt es auch spezielle Ladekabel, bei denen keine Daten durchkommen. Man darf nicht vergessen, dass beim Laden mobiler Geräte auch umgekehrt Gefahr drohen kann: Wird ein mit Trojanern infiziertes Android-Smartphone an einen PC zum Laden angeschlossen, kann der unter Umständen ebenfalls befallen werden.

„Cyberhygiene-Check-ups“. Cyber-Attacken wie Angriffe auf österreichische staatliche Infrastrukturen, Datenlecks bei politischen Parteien oder Verschlüsselungsattacken auf große Industrieunternehmen illustrieren die Gefahr, die uns alle umgibt. Das Um und Auf des Funktionierens unserer elektronischen Welt liegt in der Hand jeder Organisation und jedes Unternehmens.

Einmal im Jahr sollte in einem durch externe Spezialisten durchgeführten „Cyberhygiene-Check-up“ eine gründliche Durchuntersuchung der Computersicherheit und Datenintegrität vorgenommen werden. Die Schwachstellen sollten analysiert werden. Auf dieser Basis kann eine Liste von Verbesserungsnotwendigkeiten erstellt werden, die mit der Gesamtrisikobewertung einhergeht. Auch bei sehr sorgfältiger Vorgehensweise kann man niemals totalen Schutz vor Angriffen erreichen, diese aber dezimieren, oder schneller feststellen. Mit Software zur Prävention von Datenlecks kann beispielsweise der Abfluss von Daten entdeckt werden, bevor Hacker große Mengen stehlen können. Für Notfälle muss man aber immer gerüstet sein: Neben der schnellen Abschaltung und Abschottung betroffener Systeme kann es notwendig sein, ein elektronisches Notsystem in Betrieb zu nehmen, oder für eine Weile ohne die Verwendung von elektronischen Hilfsmitteln auszukommen. Die aktive und schnelle Kommunikation an die Mitarbeiter und Kunden – auch über papierbasierte Kanäle – und die schnelle Reaktion machen aus Opfern von Cyberkrisen respektierte Organisationen, die gelernt haben, nicht nur mit den neuen Informations- und Kommunikationstechnologien sondern auch mit den mit ihnen einhergehenden digitalen Problemen umzugehen. *Cornelius Granig*

Tipps für mehr Sicherheit unter www.darknet.help sowie unter www.bundeskriminalamt.at

Über den Autor:
Dr. Cornelius Granig leitet die Bereiche Cybersecurity und Compliance-Technologie beim internationalen Beratungsunternehmen Grant Thornton. Davor war er im Vorstand großer Banken und Versicherungen und im Management der internationalen Technologiekonzerne IBM und Siemens tätig. Im April 2019 veröffentlichte er im Kremayr & Scheriau-Verlag das Fachbuch „Darknet: Die Welt im Schatten der Computerkriminalität“.