Cyberkriminalität: reale Gefahren und griffige Massnahmen

Mit der Digitalisierung entstehen auch neue Risiken und Bedrohungen. Die Nutzenden tragen daher eine Mitverantwortung für die Sicherheit ihrer Systeme und Daten. Der konsequente Schutz von Endgeräten und ein sicherheitsorientiertes Verhalten tragen dazu bei, Systeme vor Angriffen zu schützen und sensible Daten sicher zu bewahren. Dieser Beitrag gibt eine Übersicht über Angriffsmethoden und Schutzmassnahmen.

LUCAS SCHULT
Leiter IT (CIO), Geschäftsführer, Health Info Net AG, Seidenstr.4, CH-8304 Wallisellen,
lucas.schult@hin.ch, Tel.: +41 (0)52 235 02 70, www.hin.ch

Cyberangriffe auf das Gesundheitswesen

Weltweit steht das Gesundheitswesen vermehrt im Visier von Cyberangriffen. Institutionen und Akteure des Gesundheitswesens sind oftmals immer noch nicht ausreichend geschützt und bieten deshalb ein eher einfaches Ziel. Da es bei Angriffen auf Spitäler und vergleichbare Institutionen (beispielsweise mit einem Verschlüsslungstrojaner) um sensitive Daten geht und diese Angriffe unter Umständen sogar Leben aufs Spiel setzen können, sind viele Betroffene schnell bereit, ein Lösegeld zu bezahlen, damit sie wieder Zugang zu ihren Daten erhalten und der Betrieb möglichst schnell wieder aufgenommen werden kann.[1]

Welch gravierende Auswirkungen ein Angriff im Gesundheitswesen haben kann hat das Beispiel des «Wanna Cry»-Angriffs im Jahr 2017 gezeigt. Diese Schadsoftware - eine Kombinationen von Ransomware und Wurm - nutzte eine Schwachstelle in Windows-Servern aus, um sich auf Geräten einzuschleusen und zu vermehren. Neben vielen grossen Unternehmen wie FedEx oder Renault wurde auch der britische National Health Service (NHS) mit mehreren Krankenhäusern Opfer dieses Angriffes. In der Folge konnten Rettungsstellen nur eingeschränkt arbeiten, mussten Operationen verschoben werden und war der Zugriff auf PatientInnendaten nur teilweise möglich. Dennoch sind die Spitäler mit einem blauen Auge davongekommen: Der Angriff hat keine Todesopfer gefordert.[2]

Da Cyberangriffe immer ausgefeilter werden, reicht es nicht mehr, die elektronische Kommunikation und sensitive Daten nur durch Verschlüsselung zu schützen. Der Schutz von Endgeräten und insbesondere ein risiko- bzw. sicherheitsbewusstes Verhalten - sog. Awareness - der Nutzenden spielen eine zentrale Rolle.

Unterschiedliche Geräte – unterschiedliche Risiken

Vom Kühlschrank über das Fitnessarmband bis zur smarten Glühbirne: Es gibt kaum noch eine Kategorie von elektronischen Geräten, die nicht in ein Netzwerk eingebunden werden kann. Die sogenannten Internet-of-Things-Geräte (IoT-Geräte) kommunizieren untereinander via Internet und stellen sich gegenseitig Informationen zur

Verfügung. IoT-Geräte bieten den Nutzenden oft in vielerlei Hinsicht einen Mehrwert, allerdings entstehen dabei auch neue Risiken und Angriffsflächen.

Bereits heute existieren mehr IoT-Geräte als Menschen und ihre Anzahl nimmt stetig zu. Sicherheitsrisiken entstehen, weil solche Geräte oft nur unzureichend oder gar nicht geschützt werden. Diese Sicherheitslücken bei IoT-Geräten werden oft genutzt, um darüber kritische Infrastrukturen anzugreifen. Doch auch die Daten, welche durch IoT-Geräte gesammelt und teilweise auch ausgewertet werden, können von finanziellem Interesse sein. Ein gutes Beispiel dafür sind Fitnessbänder, Smartwatches und ähnliche Geräte. Diese sogenannten «Wearables» sammeln nicht nur Daten zur Pulsfrequenz und sportlichen Aktivität, sondern setzen diese Daten auch mit Zeit und Ort in Verbindung.

Auch im medizinischen Bereich werden immer mehr Geräte mit dem Internet verbunden. Wenn im Operationssaal oder auf der Intensivstation Apparate infolge von Cyberangriffen ausfallen oder Fehlfunktionen aufzeigen, kann dies die Gesundheit und das Leben der PatientInnen gefährden.[3]

Häufige Angriffsmethoden

Um sich widerrechtlich Zugang zu Geräten und Daten zu verschaffen, werden zahlreiche Methoden verwendet. Im Folgenden soll eine Auswahl häufig genutzter Arten der illegalen Datengewinnung erläutert werden.

Schadsoftware
Mithilfe von Schadsoftware (engl.: malware), welche in das Computersystem eingeschleust wird, verschaffen sich Angreifer Zugang zu Daten.
Wird für einen Angriff bspw. Ransomware (engl. ransom, «Lösegeld») verwendet, werden die Daten auf dem Arbeitsgerät verschlüsselt und die/der BesitzerIn des Geräts kann nicht mehr auf die eigenen Daten zugreifen. In diesem Fall werden die Betroffenen meist aufgefordert, ein Lösegeld zu bezahlen, damit ihre Daten wieder entschlüsselt werden. Spyware (engl. spying, «spionieren») installiert sich meist unbemerkt auf dem Arbeitsgerät. Ziel dieser Art von Malware ist es, an Passwörter, Kontoangaben und andere sensible Daten, zu gelangen.

Phishing
Ziel des Phishings ist es, mithilfe von gefälschten E-Mails, Webseiten oder Kurznachrichten an persönliche Informationen zu gelangen und diese im Rahmen eines Identitätsdiebstahls zu verwenden. Folgen des Phishings können je nach Art der gewonnen Informationen bspw. die Plünderung eines Kontos oder der Missbrauch einer Kreditkarte sein.

DDoS (Distributed Denial of Service)
Der DDoS-Angriff ist eine gezielte und dezentral gesteuerte Attacke auf die Infrastruktur und die Netzwerke von Unternehmen, Webseiten und staatlichen Organisationen. Ziel eines solchen Angriffs ist es, durch ein enormes Mass an Anfragen und Angriffen eine Überlastung von Webseiten oder Diensten zu erzeugen, die deren Benutzung verunmöglicht. Somit steht hier die Verfügbarkeit des Systems im Fokus des Angreifers.

0day-Angriff
Der sog. 0day-Angriff (engl. zero day, «null Tage») nutzt Sicherheitslücken in Soft- oder Hardware aus, bevor dementsprechende Sicherheitsupdates oder Schutzmassnahmen zur Verfügung stehen. Solche Angriffe erfolgen in der Regel am selben Tag, an dem die betreffende Sicherheitslücke entdeckt wurde.[4]

Täter – wer steckt hinter einem Angriff?

Kriminelle Gruppierungen
Eine substanzielle Gefahr geht von kriminellen Organisationen aus.[5] Diese haben es zumeist auf Unternehmen oder Organisationen aber auch

auf Privatpersonen abgesehen, sei es um an deren Geldmittel oder an ihre Daten zu gelangen – wobei in letzterem Fall die gewonnenen Daten meist wiederum in finanzieller Absicht verwendet werden. Die Angriffe sind meist als Phishing, Malware oder DDoS zu klassifizieren.

Insider
Insider können für Regierungen, Firmen oder Organisationen eine Bedrohung darstellen. Motive können Whistleblowing, Geld (z. B. beabsichtigter Weiterverkauf von Daten), aber auch persönliche Rache sein. Angriffe können z. B. durch Missbrauch eigener Berechtigungen, Malware oder Social Engineering erfolgen.[6]

Hacktivisten
Auch Protestgruppen nutzen Cyberangriffe zur Durchsetzung ihrer Ziele. Angriffsziele sind meist Regierungen oder politische Organisationen. Ebenso wie kriminelle Organisationen nutzen Hacktivisten Phishing, Malware oder DDoS, entsprechend verschwimmen hier die Grenzen zur organisierten Kriminalität.

Script Kiddies
Eine eigene Kategorie sind Script Kiddies (auch «Skiddies»). Es handelt sich um Möchtegern-Hacker ohne vertieftes Grundlagenverständnis, die lediglich Spassmotive verfolgen oder anderen imponieren wollen, indem sie mit im Internet frei verfügbaren Tools ungeschützte Systeme angreifen. Opfer können neben Firmen und Organisationen auch Privatpersonen sein.

Schutzmassnahmen

Viele Schutzmassnahmen sind ohne grossen Aufwand umzusetzen und erhöhen den Schutz der Geräte massiv. Die wichtigsten davon lassen sich in drei Kategorien einteilen: Technische, organisatorische und verhaltensbezogene Massnahmen.

Technische Massnahmen
Zu den technischen Vorkehrungen gehört unter anderem der Schutz von Arbeitsgeräten mit einer Firewall und einem Virenscanner. Gerade Nutzende von Apple-Geräten wiegen sich hier oft in falscher Sicherheit.[7] Ausserdem ist es empfehlenswert, Updates von Betriebssystem, Webbrowser und Virenschutzprogramm immer umgehend zu installieren, um Sicherheitslücken sofort zu schliessen.

Organisatorische Massnahmen
Informationssicherheit ist Chefsache und bedingt entsprechende Vorgaben, Weisungen (z. B. bezüglich Handhabung von Daten) und Prozesse (z. B. regelmässiges Backup). Das Bewusstsein – und ein entsprechendes Verhalten – der MitarbeiterInnen hat höchste Priorität, deshalb sind regelmässige Schulungen unerlässlich. Würde bspw. die Antivirussoftware bei der Überprüfung eines E-Mail-Anhanges versagen, können dementsprechend ausgebildete Mitarbeitende grossen Schaden verhindern, indem sie den Anhang der E-Mail nicht unüberlegt öffnen.

Verhaltensregeln
Um den Zugriff Dritter auf persönliche Daten zu verhindern, ist die Verwendung von sicheren Passwörtern essentiell. Zudem ist es wichtig, dass dasselbe Passwort nicht mehrfach verwendet wird.
Bei E-Mails von unbekannten Absendern ist besondere Vorsicht geboten. Die meisten Viren kursieren in Form von E-Mail-Anhängen. Anhänge von unbekannten Absendern sollten nur mit Vorsicht oder im Zweifelsfalle gar nicht geöffnet werden.
Für die Übermittlung sensibler Daten ist die Verschlüsselung der Daten und die sichere Identifizierung des Empfängers Voraussetzung.

Endnoten

[1] Vgl. Artikel auf Global Healthcare vom 8. No- vember 2018: www.tinyurl.com/y6k4sxh6, Zugriff 2.04.2019.

[2] Vgl. Artikel auf NZZ Online vom 18. Mai 2017: www.tinyurl.com/knw8oh3, Zugriff 2.04.2019.

[3] Vgl. Artikel auf ZDNet vom 15. März 2018: www.tinyurl.com/y2gcrghn, Zugriff 02.04.2019.

[4] Vgl. Beitrag auf dem Blog «Schneider on Security» vom 17. Januar 2019: www.tinyurl. com/y7tspa9l, Zugriff 02.04.2019.

[5] Vgl. dazu die Studie «Internet organised crime threat assessment 2018» von Euro- pol: www.tinyurl.com/y2p6m9po, Zugriff 02.04.2019.

[6] Hinweise der Melde- und Analysestelle MELANI zu Social Engineering: www.tinyurl. com/y25qojjz, Zugriff 02.04.2019.

[7] Vgl. Beitrag auf heise online vom 26. Juli 2017: www.tinyurl.com/y2g8ktsa, Zugriff 02.04.2019.