Das Gesundheitswesen ist ein leichtes Ziel für Hacker

In einem Spital herrschen die wohl schwierigsten Bedingungen für die IT, die man sich vorstellen kann: Öffentlich zugängliche Bereiche, Schichtbetrieb, hohe Fluktuation der Mitarbeitenden, zertifizierte Gerätschaften mit bekannten Sicherheitslücken und zunehmender politischer Druck aufs Gesamtbudget. Das eröffnet **Hackern** ein Paradies für mögliche Angriffsziele. Wir zeigen Ihnen aus unserem Alltag greifbare Ansätze, um es Hackern ein ganzes Stück schwieriger zu machen.

▶ FABIO POLONI

Wir werden normalerweise gerufen, bevor etwas passiert. Als Ethical Hacker gehen wir zu Kunden und prüfen die unterschiedlichsten Umgebungen. Getestet werden Programme, Computer, Server, ganze Netzwerke und sogar die Mitarbeitenden. Dabei simulieren wir realistische Angriffe auf die Umgebung, finden dadurch Sicherheitslücken und fassen diese in einem Bericht zusammen. So können diese geschlossen werden, bevor ein böswilliger Hacker diese für seine Zwecke ausnutzt.

Hacker nutzen Gutgläubigkeit und Neugier

In unserem eigenen Labor kultivieren wir digitale Virenstämme. Viren hören sich erst mal an wie ein Erreger für Computererkrankungen, doch sie sind nichts anderes als kleine Programme, die von Weitem betrachtet eigentlich ganz harmlos aussehen. Ein Hacker nutzt neben technischen Sicherheitslücken auch die Gutgläubigkeit und Neugier seiner Opfer aus, um sie hinterlistig dazu zu bringen, diese schädlichen Programme auszuführen. Über diesen Weg bekommt er Zugriff auf den Computer und kann so Informationen entwenden oder den Computer fernsteuern. Testweise tun wir das auch mit den Computern unserer Kunden.

Backups und Virenscanner gegen Trojaner

Wie die Grippe, kommen auch Angriffe in Wellen. Seit geraumer Zeit sehr beliebt bei Kriminellen sind Verschlüsselungs-Trojaner. Wie der Name schon sagt, verschlüsseln sie so viele Daten wie möglich und verlangen dann Lösegeld - bezahlbar über digitale Währungen. Über die Verschlüsselung hinaus richten diese lästigen Programme in der Regel nur geringen Schaden an. Mit regelmässigen Backups Ihrer Daten und Updates der Systeme und Virenscanner kann man diesem Problem entgegenwirken und hat im Ernstfall eine Sicherungskopie bereit.

IT-Sicherheit darf kein Tabuthema sein

Tabuthemen anzusprechen ist eine Frage der Kultur. Gerade beim Thema Sicherheitsbewusstsein sprechen wir immer von einer «Sicherheitskultur». Wenn Mitarbeitende einen Verdacht haben, muss dieser von der IT ernst und dankbar entgegengenommen werden. Ansonsten werden sich die Mitarbeitenden künftig mehrfach überlegen, ob sie ihren Verdacht nun melden sollen oder nicht. Das Gleiche gilt, wenn jemand einen Fehler macht und beispielsweise auf eine Phishing-Mail hereinfällt. Wird die Person bestraft, verheimlicht sie das Missgeschick beim nächsten Mal – und die Kolleginnen und Kollegen werden das Gleiche tun. IT-Sicherheit darf kein Tabuthema sein. Man soll offen darüber sprechen, bestehende Lösungen hinterfragen und vor allem mit gutem Beispiel vorangehen.

Gefahr durch USB-Sticks und Netzwerkdosen

Die Übertragungswege von digitalen Viren sind vielfältig. Die Angreifer verschaffen sich nicht ausschliesslich über E-Mail und Browser Zugang. Es gibt USB Sticks, die automatisch Schadprogramme auf nicht gesperrten Geräten installieren. Dazu muss ein Hacker nur den richtigen Moment abwarten, den Stick am Gerät einstecken und wenige Sekunden später hat dieser über eine virtuelle Tastatur den Schadcode installiert. Alternativ werden öffentlich zugängliche Netzwerkdosen verwendet. Oft gewähren diese den direkten Zugang ins Netzwerk.

Die Virulenz eines Cyber-Ebola ist einzigartig. Aufgrund der stetigen Ver- ▸▸

besserung der Antiviren-Produkte sind die Angreifer je länger je mehr gezwungen, spezifischen Schadcode für Angriffe zu erstellen. Das heisst, eine Mutation eines bekannten trojanischen Pferdes zu erstellen, wofür noch kein Gegenmittel vorhanden ist. Bekommt der Angreifende damit Zugriff, startet er seine Erkundungsphase vom infizierten Computer aus. Im schlimmsten Fall hat der betroffene Benutzer administrative Rechte und es ist ein Leichtes, damit Informationen zu entwenden und auf andere Computer zuzugreifen. Oft finden wir auf unseren Erkundungstouren durch fremde Netze, Passwörter auf geteilten Laufwerken. Hin und wieder profitieren wir auch davon, dass die IT Administratoren mit ihren Zugangsdaten direkt auf Computer zugreifen und wir uns damit selbst als Administrator ausgeben können. Generell kann man sagen, je mehr Rechte, desto interessanter das Ziel.

> Je mehr Rechte ein User hat, desto interessanter ist das Ziel für Hacker.

Vorsicht bei Standardeinstellungen

Isolationsräume schränken die Ausbreitung ein. Sind Angreifer einmal im internen Netz, können sie mit einfachen Mitteln weitere Server und Dienste finden. Durch den Einsatz von Firewalls kann der Aktionsradius eines Angreifers jedoch effektiv eingeschränkt werden. Dies bewirkt nicht nur eine langfristig erhöhte Sicherheit, sondern resultiert auch in besserer Wartbarkeit des Netzwerks. Individuelle Behandlungsmethoden sind effizienter. Werden neue Komponenten in einem Netzwerk in Betrieb genommen, vertraut man gerne auf die Standardeinstellungen des Herstellers. Doch diese sind meistens nicht auf Sicherheit ausgelegt, sondern dafür konzipiert, in den vielen unterschiedlichen Umgebungen möglichst wenig Probleme zu verursachen. Ausserdem werden Standardeinstellungen aus Kompatibilitätsgründen nur sehr ungern gewechselt, weshalb es sich auch bei bestehenden Produkten empfiehlt, gelegentlich die Einstellungen durchzugehen und auf heutige Bedürfnisse und Standards anzupassen. Das Bewusstsein über die unterschiedlichen Einstellungen erhöht das Verständnis der Systeme und deren Interaktion.

Fabio Poloni ist gelernter Informatiker und spezialisiert auf IT Sicherheit, Notfallunterstützung und digitale Forensik. Für seine Arbeitgeberin Compass Security hackt er sich auf Kundenwunsch in Applikationen und Netzwerke, veröffentlicht gefundene Schwachstellen, löst Hacker-Rätsel und hält Vorträge zum Thema Ethical Hacking.

Die Top-Sicherheitstipps

- **Das ABC der IT Security: Prävention, Detektion, Reaktion.** Die Angriffe erfolgen heute in der Regel gegen den Computer eines Mitarbeitenden. Versuchen Sie die Computer möglichst gut gegen externen Einfluss zu schützen. Filtern Sie Schadcodes in Mails und beim Surfen, detektieren Sie Angriffe auf den Computern und im Netzwerk mit Schutzprogrammen und: Haben Sie einen Plan für den Fall der Fälle.
- **Entwickeln Sie eine Sicherheitskultur.** Sprechen Sie über IT Sicherheit und hinterfragen Sie bestehende Lösungen. Nehmen Sie Bedenken und Probleme Ihrer Mitarbeitenden ernst und seien Sie dankbar, dass Sie gemeldet werden. Wo gearbeitet wird, passieren Fehler.
- **Vergeben Sie nur die allernötigsten Rechte.** Benutzer mit vielen Rechten stellen ein wertvolles Ziel bei einem Angriff dar. Reduzieren Sie Zugriffe zwischen Netzen. Ein Computer aus dem HR muss nicht zwingend Zugriff auf Daten aus der Radiologie haben.
- **Regelmässige Backups und Updates.** Im Ernstfall verlieren Sie nur Zeit. Backups wiederherzustellen, sollte jedoch im Vorfeld geübt werden. Übrigens: Systeme, die regelmässig aktualisiert werden, sind auch in Zukunft leichter zu aktualisieren, da weniger Änderungen vorgenommen werden.
- **Misstrauen Sie dem Bildschirm und den Displays und sichern Sie Schnittstellen.** Daten, die Ihnen ungefragt zugespielt werden, auch von vermeintlich vertrauenswürdigen Quellen, können infiziert sein. Angreifer schicken SMS und E-Mails mit gefälschtem Absender. Das ist für ein Profi etwa so einfach, wie wenn Sie einen Brief mit falschem Absender verfassen müssten. Auch die Anzeige von Telefonnummern kann manipuliert werden. Schützen Sie zudem öffentlich zugängliche Schnittstellen wie USB- und Netzwerkanschlüsse.
- **Passwörter sind Privatsache.** Passwörter sollen nie ausgesprochen oder aufgeschrieben werden. Weder auf einer Heftnotiz unter der Tastatur, noch in einer gemeinsamen Excel-Tabelle. Verwenden Sie für jeden Dienst und jedes Gerät ein anderes Passwort. Etablieren Sie dafür einen digitalen Passwort-Safe.