Cyber-Sicherheit

Medizingeräte vor Hackern schützen

In der SRF-Sendung Rundschau über Cyber-Angriffe auf Spitäler ist die Problematik nur symptomatisch aufgezeigt worden. Der Gesamtverantwortliche für Informationssicherheit am Universitätsspital Zürich, Erik Dinkel, und der Berufs-Hacker Nicolas Mayencourt, zeigen nun Lösungen auf. Dringenden Handlungsbedarf orten sie bei den Medizingeräten.
Interview von Martina Greiter

Die Sendung Rundschau von SRF zum Thema Cyber-Attacken zeigte Anfang 2020 auf, wie verwundbar die Schweizer Spitäler sind.
NM: In der Sendung wurde nur die Verwundbarkeitsstudie diskutiert, für die wir in 281 Spitälern die IT-Sicherheit geprüft haben. Es kamen leider nur die Symptome zur Sprache, nicht aber die Ursachen und die Lösungsansätze. Ja, wir haben Sicherheitsprobleme festgestellt. Wir sind mit den betroffenen Spitälern in Kontakt und klären gemeinsam, wie sie die Sicherheit verbessern können. Wenn sie die entsprechenden Massnahmen umsetzen, wird die IT der betroffenen Spitäler sicherer. Es bestehen in Spitälern jedoch – vereinfacht gesagt – zwei IT-Bereiche: Ein Büronetzwerk mit den gängigen Anwendungen, wie wir sie in allen Firmen finden: E-Mail, Datenbanken, Dokumentenablage. Und zusätzlich gibt es den Bereich mit den Medizingeräten. Dieser ist, mit gutem Grund, stark reguliert. Die Hersteller müssen strenge Sicherheitsnormen erfüllen, damit die Geräte überhaupt zugelassen werden.

Und trotzdem sind die Spitäler bei den Medizingeräten angreifbar?
ED: Lassen Sie mich zuerst ebenfalls zum Rundschaubericht Stellung nehmen, bevor ich Ihre Frage beantworte. Informationssicherheit besteht aus verschiedenen Sicherheitsringen. Die in der Sendung erwähnte Studie beschränkte sich auf den ersten Ring. Eine generelle Aussage über die Informationssicherheit eines Spitals ist daher nur bedingt möglich. Zudem entsteht aus dem Rundschaubericht der Eindruck, Spitäler in der Schweiz seien generell unsicher, was klar falsch ist. Wir haben es heute mit hoch professionellen Cyber-Kriminellen zu tun, welche über ein Milliardenbudget verfügen und teilweise sogar staatlich geduldet oder gesponsert werden. Entsprechend nehmen die Professionalität und Anzahl der Angriffe zu. Gleichzeitig steigt durch die fortschreitende Digitalisierung die Abhängigkeit von der IT und damit die Verletzlichkeit eines Spitals. Dieser grossen Herausforderung tragen die Spitäler Rechnung und optimieren die Informationssicherheit laufend. Früher war deren Gewährleistung verhältnismässig einfach. Ein Spital musste den Perimeter im Griff haben; ähnlich einer Burgmauer. Die einzigen Verbindungen gegen aussen waren E-Mail und Internet.

Heute kommen Mobile Devices, Cloud-Lösungen und Remote Working hinzu sowie zunehmend auch Medizingeräte, welche in das IT-Netzwerk integriert sind und teilweise sogar von extern für Supportzwecke erreicht werden können. Einfach eine Mauer um die Burg zu bauen, reicht schon lange nicht mehr. Die Informationssicherheit eines Spitals muss auch die Medizingeräte abdecken. Dass aber gerade bei diesen den Spitälern wegen Abhängigkeiten von den Herstellern oft die Hände gebunden sind, kam im Rundschaubericht leider nicht zur Sprache.

Inwiefern?
NM: IT-Systeme im Büronetzwerk eines Spitals werden regelmässig geprüft und aktualisiert. Die Geräte im medizinischen Bereich hingegen werden einmal geprüft, kriegen die Markzulassung und dürfen danach nicht mehr verändert werden. Die

Foto: Dreamlab Technologies

«Die Medizingeräte werden einmal geprüft, kriegen die Markzulassung und dürfen danach nicht mehr verändert werden. Die Prüfungsschemata für die Zulassung sind veraltet.»

Nicolas Mayencourt

Prüfungsschemata für die Zulassung sind veraltet. Sie waren noch vor ein paar Jahren gut genug, da damals jedes Gerät eine Software hatte, die eigens für dieses Gerät hergestellt worden war. Heute ist das anders.

Was hat sich denn beim Aufbau der medizinischen Geräte verändert?
NM: Wir meinen, dass es Spezialgeräte sind. Sie bestehen jedoch aus generischen Software- und Hardware-Komponenten, also aus den gleichen Bauteilen wie etwa Fernseher, Laptops oder Autosteuerungen. Und sie haben die gleichen Sicherheitsrisiken. Was auf einem Laptop ein tolerierbares Risiko sein mag, ist jedoch bei einem medizinischen Spezialgerät unter Umständen lebensgefährlich.

Was bedeutet das für die Spital-IT?
NM: Dass veraltete Systeme mit bekannten Schwachstellen im Einsatz sind, die ein grosses Risiko darstellen.

Aber die Geräte wurden doch nach strengen Regeln geprüft und offiziell zugelassen?
ED: Medizingeräte werden als solche zertifiziert. Danach dürfen sie nicht mehr verändert werden. Das bedeutet, dass weder der Hersteller noch wir als Spital Updates durchführen können. Ebenso wenig kann auf einem solchen Gerät ein Antivirenprogramm betrieben werden, da ein solches tägliche Updates erfordert. Oder wenn eine Software durch den Gerätehersteller nicht weiterentwickelt wird und mit neuen Betriebssystemen nicht kompatibel ist, steht das Spital vor der Wahl, die Software für Behandlung und/oder Forschung nicht mehr zu nutzen oder die Software auf einem Computer mit einem veralteten Betriebssystem zu betreiben und die damit verbundenen Risiken zu tragen.

NM: Medizingeräte bestehen heute im Wesentlichen aus einer Standard-Hardware-Plattform und einem Standardbetriebssystem – das ist natürlich auch vermeintlich kosteneffizient für die Hersteller.

Warum ist das ein Problem?
NM: Diese Standardbauteile sind so konzipiert, dass sie auf allen Geräten laufen und möglichst viele Funktionen unterstützen, damit man sie für alle möglichen Zwecke einsetzen kann. Sie haben viel mehr Funktionen als Medizingeräte benötigen. Etliche Schnittstellen zur Aussenwelt, über die etwas ein- oder ausgegeben werden kann, bieten eine grosse externe Angriffsfläche. Die Spitäler müssen diese zertifizierten und zugelassenen Spezialgeräte während Monaten oder sogar Jahren ohne Sicherheitspatches mit dem an sich korrekt gewarteten Office-Netzwerk und damit auch indirekt mit dem offenen Internet verbinden – dadurch wird auch die Sicherheit des Office-Netzwerks stark gefährdet.

Warum wird die Sicherheit der Spezialsysteme nicht durch Patches erhöht?
ED: Wenn wir ein zertifiziertes Medizingerät verändern, würde das Gerät seine Zertifizierung verlieren und dürfte nicht mehr betrieben werden. Der Hersteller würde keinerlei Garantie übernehmen und keinen Support leisten. Die Spitäler können zwar Sicherheitsmassnahmen im Office-Netzwerk umsetzen, z. B. indem sie dieses in Zonen und Segmente unterteilen, was jedoch kaum Einfluss auf die Sicherheit der Medizingeräte hat.

NM: Ein Spital arbeitet mit besonders schützenswerten Personendaten und ist gesetzlich dazu verpflichtet, diese zu schützen. Veraltete Systeme gefährden die Vertraulichkeit dieser Daten stark. Das ist aber noch nicht das Schlimmste: Die Angriffe mit der Schadsoftware Petya/NotPetya haben 2017 eindrücklich gezeigt, wie eine Ransomware in Windeseile ganze Spitäler lahmlegen und dass dies auch zu Personenschäden führen kann.

Würde die Sicherheit verbessert, wenn Spezialgeräte regelmässig mit Patches gewartet werden könnten?
NM: Patches würden die Sicherheit erhöhen. Aber das reicht natürlich noch nicht. Die Sicherheit würde sich deutlich verbessern, wenn die medizinischen Geräte anstelle von Standartkomponenten mit sogenannten Specific-Purpose-Systemen wie z. B. einem Mikrokernel laufen würden. Diese sind nur mit ganz wenigen Funktionalitäten bestückt – mit genau denjenigen, die für den Betrieb von solchen Geräten notwendig sind. Wenn nur solche spezifischen Bauteile eingesetzt würden, wäre der Aufwand zur Gewährleistung der Sicherheit viel geringer, auch die Angriffsfläche wäre kleiner. Eine andere Möglichkeit ist es, die verbauten Komponenten und das System zu härten und in ihrer Funktionalität so stark einzuschränken, dass sie betriebssicher sind.

Was sollte konkret getan werden, um die Sicherheitssituation zu verbessern?
ED: Die Hersteller müssen zwingend Verantwortung übernehmen und bei der Entwicklung ihrer Medizingeräte nicht nur auf deren Funktionalität achten, sondern auch die Informationssicherheit der Geräte zeitgemäss gewährleisten. Eine Variante, wie sie von einzelnen Herstellern bereits angeboten wird, ist die Erweiterung des Gerätes mit einer Hardware Appliance, welche die fehlenden Updates und/oder die Mängel einer veralteten Software auf dem

«Die Hersteller müssen zwingend Verantwortung übernehmen und bei den Medizingeräten nicht nur auf die Funktionalität achten, sondern auch die Informationssicherheit gewährleisten.»

Erik Dinkel

Foto: Erik Dinkel

Gerät selber abfangen. Weitere Varianten hat Herr Mayencourt erwähnt. Ich möchte aber betonen, dass Informationssicherheit nicht Selbstzweck ist, sondern dazu dient, die Verfügbarkeit der Systeme und die Integrität und Vertraulichkeit der Daten zu gewährleisten. Im Zentrum steht der sichere Betrieb des Spitals und dessen Resilienz bei einem Cyber-Vorfall.

Es ist also nicht nur wichtig, das Spital vor Cyber-Angriffen zu schützen, sondern es geht auch darum, einen erfolgreichen Angriff unmittelbar zu erkennen und rasch und angemessen darauf zu reagieren. Ähnlich wie bei einem analogen Virus, müssen bei einem Cyber-Virus die infizierten Systeme möglichst früh erkannt und isoliert werden, um eine Ausbreitung auf das ganze System zu verhindern. Kommt es zu einer Ausbreitung muss die IT-Abteilung in enger Zusammenarbeit mit der Medizin weitere Massnahmen treffen, um den sicheren Betrieb des Spitals weiter zu garantieren.

«Industrie, Hersteller und Regulatoren müssen gemeinsam Lösungen finden, um die benötigte Sicherheit zu erreichen.»
Nicolas Mayencourt

Wie kann erreicht werden, dass die Gerätehersteller ihre Verantwortung wahrnehmen?
NM: Während 25 Jahren hat der Markt das Problem nicht geregelt. Die wenigen Medizingerätehersteller weltweit haben keinen Anreiz, etwas zu verändern. Dies gilt auch für die staatlichen Regulatoren. Der Leidensdruck ist noch zu klein. Es ist also wichtig, ein möglichst breites, öffentliches Problemverständnis zu schaffen.

Was ist also zu tun?
NM: Industrie, Hersteller und Regulatoren müssen gemeinsam Lösungen finden, um die benötigte Sicherheit zu erreichen. Diese Arbeit ist wichtig, da sie uns dabei hilft, die Chancen der Digitalisierung verantwortungsvoll zu nutzen. Wir haben alle ein grosses Interesse daran, dass diese Geräte zuverlässig funktionieren!

ED: Bei der Standard-IT-Ausrüstung ist die Sicherheitslage international recht gut, mit allgemein anerkannten Standards wie ISO-Zertifikaten. Hier ist keine stärkere Regulierung notwendig. Bei den Medizingeräten besteht jedoch Handlungsbedarf. Wobei ich eine Lösung ohne zusätzliche Regulierung bevorzugen würde, welche auf die Eigenverantwortung der Hersteller setzt. Ich denke, wir sind bereits auf dem richtigen Weg. Zu nennen ist der von H+ und den Spitälern der Schweiz erarbeitete Leitfaden «Anforderungen zur ICT-Sicherheit von Fremdsystemen».

Wie wirkt sich die aktuelle Corona-Krise auf die IT-Sicherheit der Spitäler aus?
NM: Die Schweiz hat auf die Krise mit etwas Verzögerung gut reagiert, die Menschen halten sich an die Vorschriften, gerade in den Spitälern. Homeoffice funktioniert bei den meisten einwandfrei. Wenn jetzt in dieser Ausnahmesituation allerdings auch noch im IT-Bereich etwas passiert, ist das ein Problem. Da auch die IT-Mitarbeitenden im Homeoffice sind und entsprechend längere Reaktionszeiten haben oder bei einem IT-Ausfall «ausgesperrt» wären. Es gibt zudem bereits Malware, Phishing-Angriffe und Trojaner, die sich z. B. als Corona-Infos tarnen und auch Spitäler treffen. Es gilt also auch gegenwärtig wachsam zu sein. Wir werden aber auch viel daraus lernen.

ED: Die Bedrohung hat sich im Grundsatz durch die Corona-Krise nicht verändert und die bisherigen Sicherheitsmassnahmen sind weiter wirksam. Was aber zugenommen hat, ist die Verwundbarkeit der Spitäler. Ein erfolgreicher Cyber-Angriff wäre in der aktuellen Lage fatal. Leider schrecken Cyber-Kriminelle nicht davor zurück, die Situation auszunutzen und verschicken z. B. gefälschte E-Mails im Namen des BAG, welche Schadsoftware enthalten.

Am Universitätsspital Zürich (USZ) haben wir daher die Mitarbeitenden entsprechend sensibilisiert. Auch was das Homeoffice betrifft, sind wir am USZ gut aufgestellt. Zentral ist die Verwendung sicherer Verbindungen wie z. B. VDI oder VPN in Kombination mit einer Mehr-Faktor-Authentisierung (MFA) zur Anmeldung.

Unabhängig von der Corona-Krise nimmt die Abhängigkeit der Spitäler von der IT signifikant zu und damit auch die Verletzlichkeit vor Cyber-Angriffen. Dem gilt es Rechnung zu tragen und die Informationssicherheit in einer dezentralen und heterogenen Systemlandschaft auch gemeinsam mit den Herstellern von medizintechnischen Produkten sicherzustellen. ■

Erik Dinkel, Chief Information Security Officer (CISO), Universitätsspital Zürich (USZ);
erik.dinkel@usz.ch

Nicolas Mayencourt, Gründer und Geschäftsführer, Dreamlab Technologies, Bern;
contact@dreamlab.net

Piratage informatique: il faut agir vite

L'émission Rundschau de la télévision alémanique s'est intéressée au début de l'année aux cyberattaques dans les hôpitaux. Mais elle n'a mis le doigt que sur les symptômes de la problématique. Erik Dinkel et Nicolas Mayencourt présentent ici des pistes de solution.

Les appareils médicaux sont testés une fois, obtiennent la validation nécessaire et ne peuvent ensuite plus être modifiés. Cela signifie que ni les fabricants ni les hôpitaux ne peuvent faire de mises à jour, souligne Erik Dinkel. De même, l'utilisation de programmes antivirus est très limitée sur de tels équipements. En outre, si un software n'est plus développé par un fabricant et qu'il n'est pas compatible avec de nouveaux systèmes d'exploitation, l'hôpital a une alternative: ne plus utiliser le software ou l'utiliser sur un ordinateur fonctionnant avec un système d'exploitation dépassé, avec tous les risques y relatifs. Et si des modifications sont apportées à l'appareil, celui-ci perd sa certification.

Les fabricants doivent absolument prendre leurs responsabilités: ils doivent non seulement veiller à la fonctionnalité des appareils médicaux qu'ils développent, mais aussi en garantir la sécurité informatique. Pour mettre les fournisseurs devant leur propre responsabilité, Erik Dinkel privilégierait une solution sans réglementation supplémentaire. De son côté, Nicolas Mayencourt souligne que le problème n'a pas été réglé depuis le début, soit depuis 25 ans. En nombre réduit sur le marché mondial des dispositifs médicaux, les fabricants n'ont aucune incitation à changer quoi que soit. Et c'est vrai aussi pour les instances étatiques de régulation. La pression est encore insuffisante. Il est donc important d'intensifier et d'élargir le débat dans le public. Industrie, fournisseurs et régulateurs doivent trouver ensemble des solutions. ■

Cyber-Corona

Genau hinschauen: Halten Sie auch Ihre IT sauber!

Im März 2020 stieg die Anzahl der Phishing-Angriffe in der Schweiz um 457 Prozent. Mitarbeitende in Gesundheitsberufen sind in der COVID-19-Krise besonders im Visier von Cyberkriminellen. – *Von Nicolas Mayenencourt*

Vielleicht arbeiten Sie zurzeit wie viele andere im Homeoffice. Ein E-Mail trifft ein. Das Bundesamt für Gesundheit (BAG) schreibt: «In Ihrem Umfeld wurden COVID-19-Infektionen festgestellt». Sie werden um Hilfe gebeten. Man habe vergeblich versucht, die Betroffenen zu kontaktieren. Im Anhang ein PDF mit dem BAG-Logo. Darin findet sich ein Link, unter dem Sie die Kontaktdaten Ihrer Bekannten eingeben können. Sie klicken darauf und infizieren sich mit einer Malware, die Ihren privaten Computer bedroht und das gesamte Firmennetzwerk zerstören kann.

Die aktuelle Bedrohungslage

Vor allem Mitarbeitende in Gesundheitsberufen werden zurzeit mit E-Mails eingedeckt, die angeblich vom BAG, der WHO oder von anderen Gesundheitsdiensten stammen und Informationen zu COVID-19 beinhalten. Dabei handelt es sich oft um Phishing-Angriffe mit dem Ziel, Sie dazu zu bringen, einen Link oder Anhang zu öffnen. Wer es tut, gibt z. B. unwissentlich seine Zugangsdaten weiter, installiert Ransomware (Erpressersoftware) oder lässt eine Verbindung mit einem Command-and-Control-Server (kriminelles Botnetz mit automatisierten Schadprogrammen) zu. Das ermöglicht es Angreifern, Daten zu stehlen oder zu manipulieren. Medizinische Daten sind besonders interessant. Der Preis dafür ist auf dem Schwarzmarkt (Deep Web) rund zehnmal so hoch wie für Kreditkartendaten.

So schützen Sie sich

Ihre IT-Abteilung hat im Normalbetrieb einen Schutz nach dem Konzept «Defense in Depth» implementiert. Dieser beinhaltet mehrere Kontrollschichten. Wenn ein Angriff durch Klicken auf einen Link oder Öffnen eines Anhangs ausgelöst wird, müssen verschiedene Sicherheitsvorkehrungen überwunden werden: Ein Antiphishing-Gateway, der Firmen-Antivirusschutz, der Geräte-Virenschutz und das Firewall-Intrusion-Detection- bzw. Intrusion-Prevention-System.

Im Homeoffice sind die Schichten zwar teilweise ebenfalls aktiv. Es werden z. B. Firmenlaptops und VPN (Virtuelles Privates Netzwerk) verwendet. Aber der Angriffsbereich ist über die ganze Belegschaft verteilt und braucht daher noch grösseren Schutz. Zudem sind die Reaktionszeiten länger, da sich die IT-Sicherheitsspezialisten nicht vor Ort befinden. Umso wichtiger ist die letzte Sicherheitsschicht: Die Sensibilisierung der Mitarbeitenden. Prüfen Sie E-Mails genau, öffnen Sie Anhänge nur, wenn Sie sicher sind, dass die Nachricht echt ist. Rufen Sie z. B. den Absender an, um das zu klären.

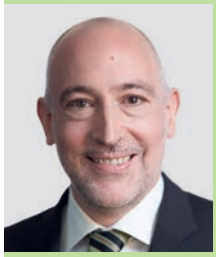
So funktionieren die Attacken

Im eingangs geschilderten Fall war der Link im PDF über einen Kurzlink-Service getarnt und führte zu einer ISO-Datei, die sich auf einer kostenlosen Hosting-Plattform befand. Die Datei beinhaltete eine Malware, die darauf angelegt ist, Informationen zu Finanztransaktionen zu stehlen. In anderen Fällen sind es Office-Dateien mit Makros, PDF- oder ZIP-Dateien, die Malware beinhalten. Deren Ziel ist Sabotage oder Erpressung.

Sicheres Homeoffice

Die Melde- und Analysestelle Informationssicherung (MELANI) bietet mehr Informationen zum Thema und Checklisten für ein sichereres Homeoffice. ■

Info: www.melani.admin.ch



Nicolas Mayencourt, Gründer und Geschäftsführer, Dreamlab Technologies, Bern; contact@dreamlab.net

Attention aussi aux virus informatiques!

En mars dernier, le nombre de tentatives de hameçonnage a augmenté de 457 % en Suisse. Les cybercriminels s'en prennent particulièrement aux professionnels de la santé, qui reçoivent moult courriers électroniques censés prozvenir de l'OMS, de l'OFSP ou d'ailleurs et contenir des informations sur le COVID-19. Les destinataires sont incités à cliquer sur un lien ou à ouvrir une pièce jointe et ils se retrouvent infectés par des logiciels malveillants, qui menacent leur ordinateur privé et peuvent détruire le réseau de leur entreprise.

En temps normal, les services informatiques des entreprises mettent en place des systèmes de sécurité multicouches, qui sont aussi partiellement actifs à domicile. Mais la protection doit être renforcée parce que la zone d'attaque est répartie sur l'ensemble des collaborateurs. En outre, le temps de réaction est allongé en raison de l'éloignement des spécialistes de la sécurité informatique. La dernière couche de protection, la sensibilisation des employés, est donc d'autant plus importante. Il est nécessaire de vérifier soigneusement ses e-mails et d'ouvrir les pièces jointes seulement si l'on est convaincu de l'authenticité de l'expéditeur. En cas de doute, il est conseillé de l'appeler pour s'en assurer. ■

Starke Zunahme der Phishing-Angriffe

Der Jahresumsatz von Cyberattacken beträgt im Schnitt ca. 1,5 Trillionen US-Dollar. Das ist doppelt so viel wie derjenige von Google, Amazon, Facebook und Microsoft zusammen. Im März 2020 stieg die Anzahl der Phishing-Angriffe in der Schweiz um 457 Prozent. ■

Info: www.govcert.admin.ch