Ungebetene Gäste in Spital-IT-Systemen lassen aufhorchen: Wie sicher sind wir in der Schweiz?

Verbrecherische Hacker: Gefahr erkannt – Gefahr gebannt?

Stellen Sie sich vor: Der Patient wird für die Operation vorbereitet, der Chirurg will die jüngsten Vitaldaten und MRI-Aufnahmen auf den Bildschirm holen, aber KIS wie PACS streiken. Die Daten sind gesperrt. Hacker waren am Werk. Das Spital hat ein grosses Problem. Exakt das ist in Deutschland und den USA bereits passiert. Erleben wir den nächsten Fall bei uns?

Aus Deutschland wurde in jüngster Zeit gleich ein halbes Dutzend Kliniken von Computerviren angegriffen, Operationen mussten abgesagt werden, Patienten blieben unversorgt. In Kalifornien wurde das System eines Spitals sogar während sechs Tagen völlig blockiert. Noch schlimmer: Alle Spitäler wurden erpresst. Genauso erging es deutschen Online-Apotheken. Das Vorgehen ähnelt sich: Mit Cryptoviren verschlüsseln Hacker die Daten der Institutionen, dann folgt ein Erpresser-Mail: Gegen eine bestimmte Summe, zahlbar in Bitcoins, erhalten die Opfer einen «Schlüssel», um ihre Daten wieder nutzen zu können. – Droht der Schweiz gleiches Übel?

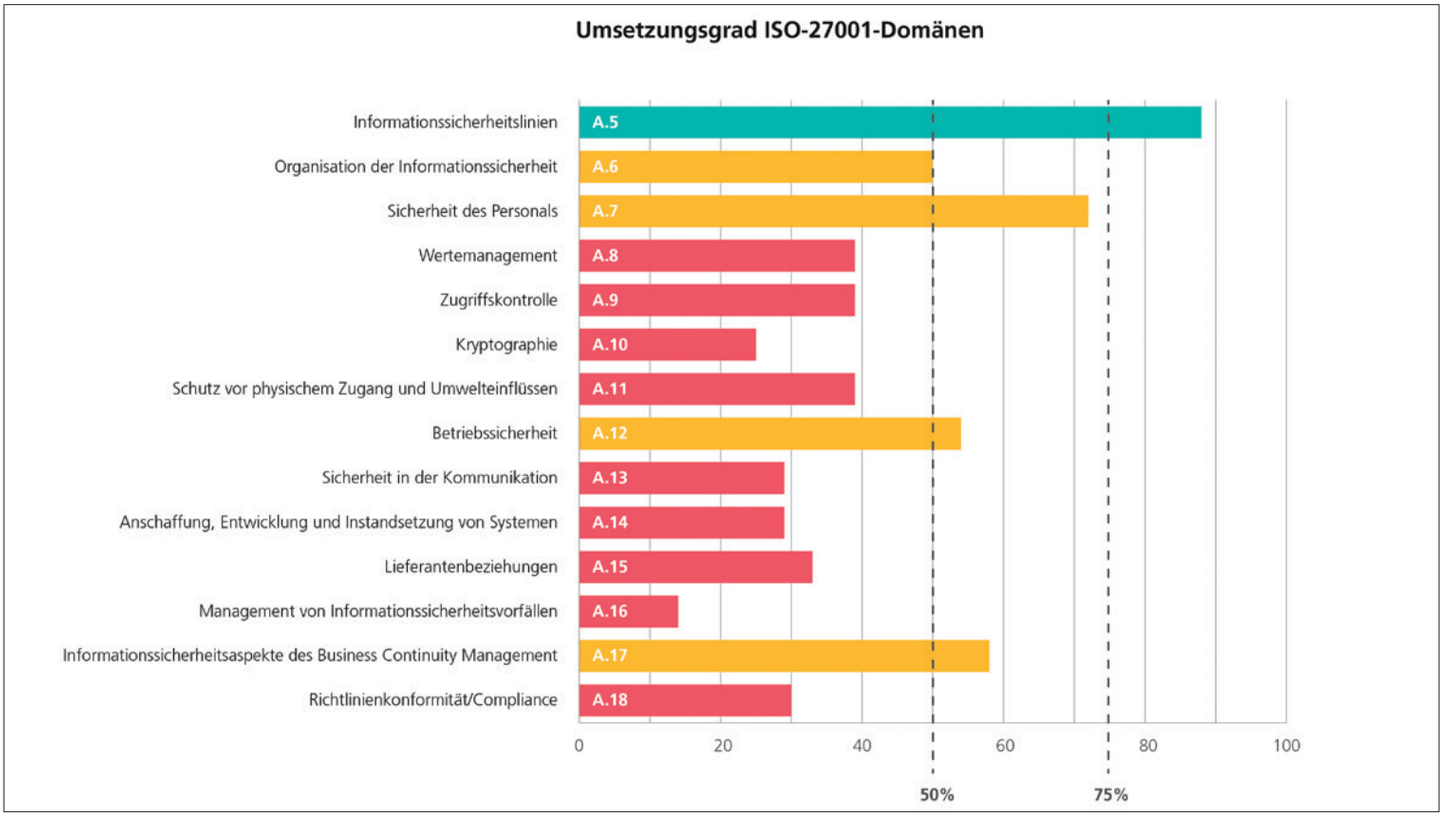
Arztpraxen gehackt

Cyberrisiken halten sich nicht an Landesgrenzen. Im Security Operation Center (SOC) der HINT AG weiss man um die Cyberrisiken und ganz besonders um die Folgen für Institutionen des Gesundheits- und Sozialwesens. Und die Gefahr ist sehr ernst zu nehmen, wurden doch unlängst Schweizer Arztpraxen gehackt.

Infiziert wurden sie durch eine spezielle Art von Viren, sog. Cryptoviren. Sie sind nicht wählerisch und befallen jedes System, zu dem sie Zugang finden. So gefährden sie die Datensicherheit auf eine Weise, die ausgesprochen schädlich ist. Und, wie es Urs Achermann, Chief Security Officer der HINT AG, trefflich ausdrückt: «Der Blitz kann überall einschlagen.»

Vorbeugen ist besser als Heilen

Cyberrisiken werden für gewöhnlich als externe Bedrohungen wahrgenommen, was nur teilweise richtig ist, weil sie der unfreiwilligen Unterstützung der IT-Systeme und sogar der Anwender bedürfen. Deshalb betreffen Cyberrisiken sowohl die Sicherheit als auch den Schutz der Daten. Stichworte dazu: Gesundheitsdaten, und



Das Security Operation Center (SOC) der HINT AG hält laufend mit den Anforderungen und den Bedrohungen der digitalen Zeit Schritt. Unser Bild zeigt eine Gesamtanalyse entscheidender Sicherheitskriterien auf einen Blick.

somit auch Patientendaten, unterstehen dem Arztgeheimnis. Als ICT-Spezialist für das Gesundheits- und Sozialwesen betreibt die HINT AG ein ständig wachsendes Security Operation Center (SOC), das laufend mit den Anforderungen und den Bedrohungen der digitalen Zeit Schritt hält. Wie hoch die Anforderungen an ein SOC inzwischen sind und wie Kunden von einer professionellen SOC-Infrastruktur profitieren können, lässt sich anhand der modernen Cyberrisiken aufzeigen.

Mit Raffinesse Millionen ergaunert

Aus US-Spitälern ist bekannt, dass wegen der Hacker-Angriffe auf beinahe steinzeitliche Arbeitsmethoden zurückgegriffen werden musste. So wurden Berichte wieder auf Papier erstellt und per Boten überbracht. Oft sind raffiniert eingeschleuste E-Mails die Ursache des Virus-Befalls und damit eines erfolgreichen Hacker-Angriffs. Noch sind die bekannt gewordenen erpressten Beträge im Verhältnis zum tatsächlich eingetretenen oder zu befürchtenden Schaden relativ gering. Trotzdem wird das innert zwei Monaten ergaunerte Lösegeld auf 325 Millionen Dollar geschätzt (Quelle: cyberthreatalliance.org). Die «BCM News» berichten, dass der Virenhersteller Bitdefender wisse, dass 50 Prozent der amerikanischen Opfer das Lösegeld in Bitcoins entrichtet haben.

Beim Öffnen von Mails ist also höchste Vorsicht am Platz. Die Angriffe sind nämlich äusserst intelligent geworden und nicht immer auf den ersten Blick als solche zu erkennen. Die Mail-Absender sprechen ihre Adressaten persönlich an und verwenden Inhalte, die – gerade im hektischen Spitalalltag – auf die Schnelle durchaus als plausibel erscheinen. Ausserdem gibt es bislang nur wenige Gegenmittel gegen Verschlüsselungen durch Ransomware, welche ganze IT-Systeme wie ein KIS lahmlegen können. Gefahr ist in Verzug. Wie gross ist sie hierzulande?

Das Risiko ist sehr ernst zu nehmen

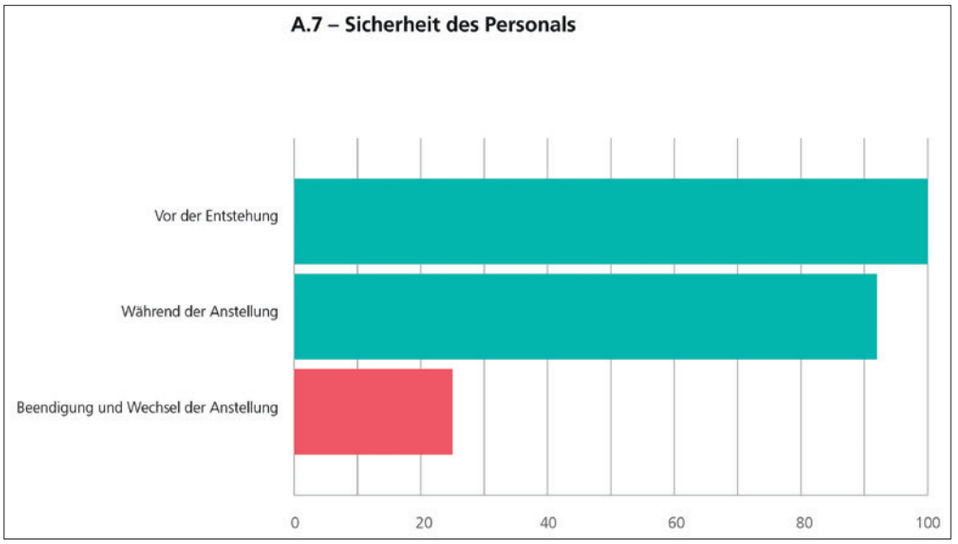
«Die Gefahr ist gross.» Diese Meinung vertritt Urs Achermann, Chief Security Officer der HINT AG. «Die von den Kriminellen eingesetzten Cryptoviren finden verschiedene Wege, um auf den Computer eines Opfers zu gelangen. Dabei sind vor allem zwei Wege üblich: via Mail mit verseuchtem Anhang (z.B. einem Word-Dokument) oder mit einem Link auf eine verseuchte Webseite. – Zweite Methode: Der Virus verteilt sich selber auf einer Webseite, die gehackt worden ist, via sog. ‹Drive-by-downloads›: Ein Mitarbeiter ruft eine bestimmte Webseite auf, liest dort einen Artikel und geht wieder weiter auf eine andere Webseite. Weil neben dem Artikel aber ein Werbebanner gehackt wurde, kann der Angreifer jetzt über eine noch nicht kommunizierte oder nicht gepatchte Sicherheitslücke auf den Computer des Mitarbeiters gelangen, ohne dass dieser etwas Böses angeklickt hat.»

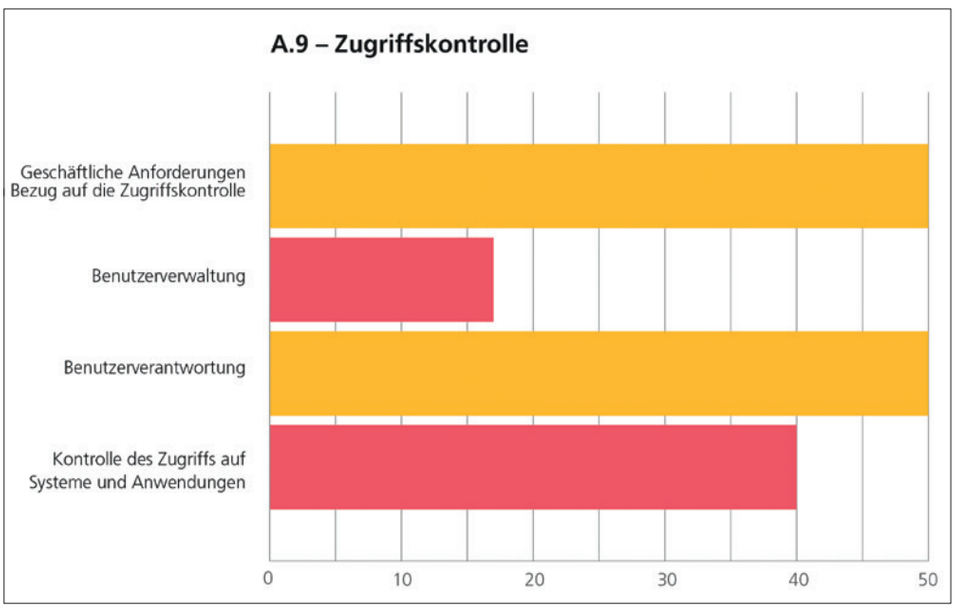
Cryptoviren: teuflische Raffinesse

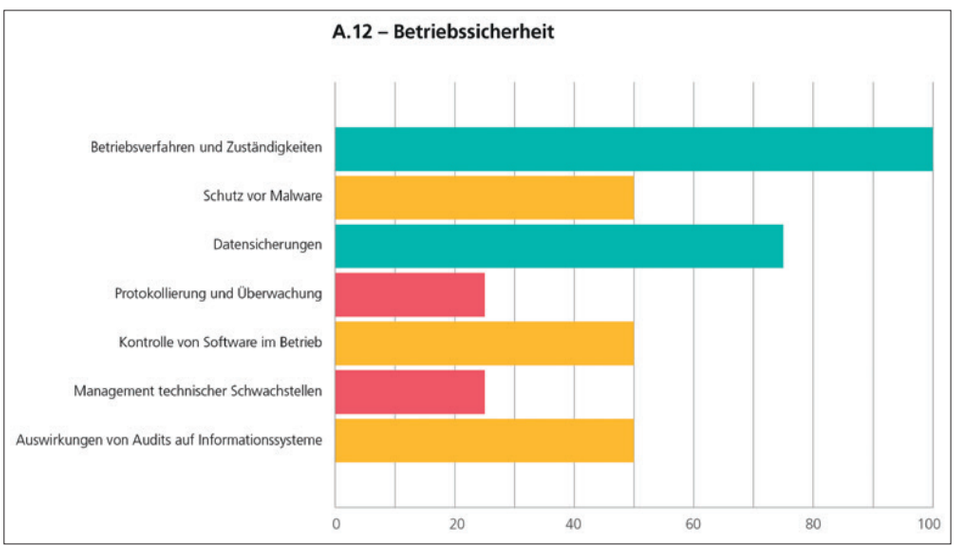
Das Einnisten der Cryptoviren geschieht auf teuflische wie systematische Art:

1. Ein Cryptovirus nimmt als Erstes auf dem angegriffenen PC Kontakt auf mit einem sogenannten «Command and Control Server» (C2C Server).
2. Hier meldet der Virus, dass er nun auf einem Zielsystem bereit sei und einen Schlüssel brauche, um Daten auf dem Zielrechner zu verschlüsseln.
3. Der C2C Server erstellt einen starken Schlüssel und übergibt ihn an den Virus auf dem Zielrechner.
4. Jetzt beginnt der Cryptovirus, alle Daten, auf die er Zugriff und Berechtigungen hat, mit diesem starken Schlüssel zu verschlüsseln.

Übersichtlich präsentieren sich die Sicherheits-Details einer Gesundheits-Institution. Wo im Ampelsystem rot eingezeichnet ist, herrscht akuter Handlungsbedarf.







5. Betroffen sind dabei primär Microsoft Office-Dokumente (Word, Excel, PowerPoint, Visio), PDF-Dateien und Bilder (JPG, PNG).
6. Wenn solche Dateien vom Hacker verschlüsselt sind, sind sie für den Benutzer nicht mehr verwendbar.

Ein betroffenes Spital kann nach einem Cryptovirus-Angriff weder verschlüsselte Word-Dokumente öffnen noch Bilder anschauen. Der Virus legt bewusst Spuren auf dem angegriffenen Computer in Form von «Hilfeseiten» und Mitteilungen, auf welchen steht, wo der angegriffene Benutzer wieviel Lösegeld bezahlen muss, um wieder an seine Daten zu gelangen. Die Viren selber sind professionell programmiert, verändern sich konstant, verwenden richtig starke Schlüssel und verstecken sich selber sehr geschickt auf dem angegriffenen Rechner. Um einmal verschlüsselte Dateien wieder «brauchbar» zu machen, brauchen Betroffene unbedingt den geheimen Schlüssel, um damit alle Dateien zurück in den Ursprungszustand bringen.

Warum kann man Applikationen und Systeme nach einem Crypto-Angriff nicht mehr nutzen?

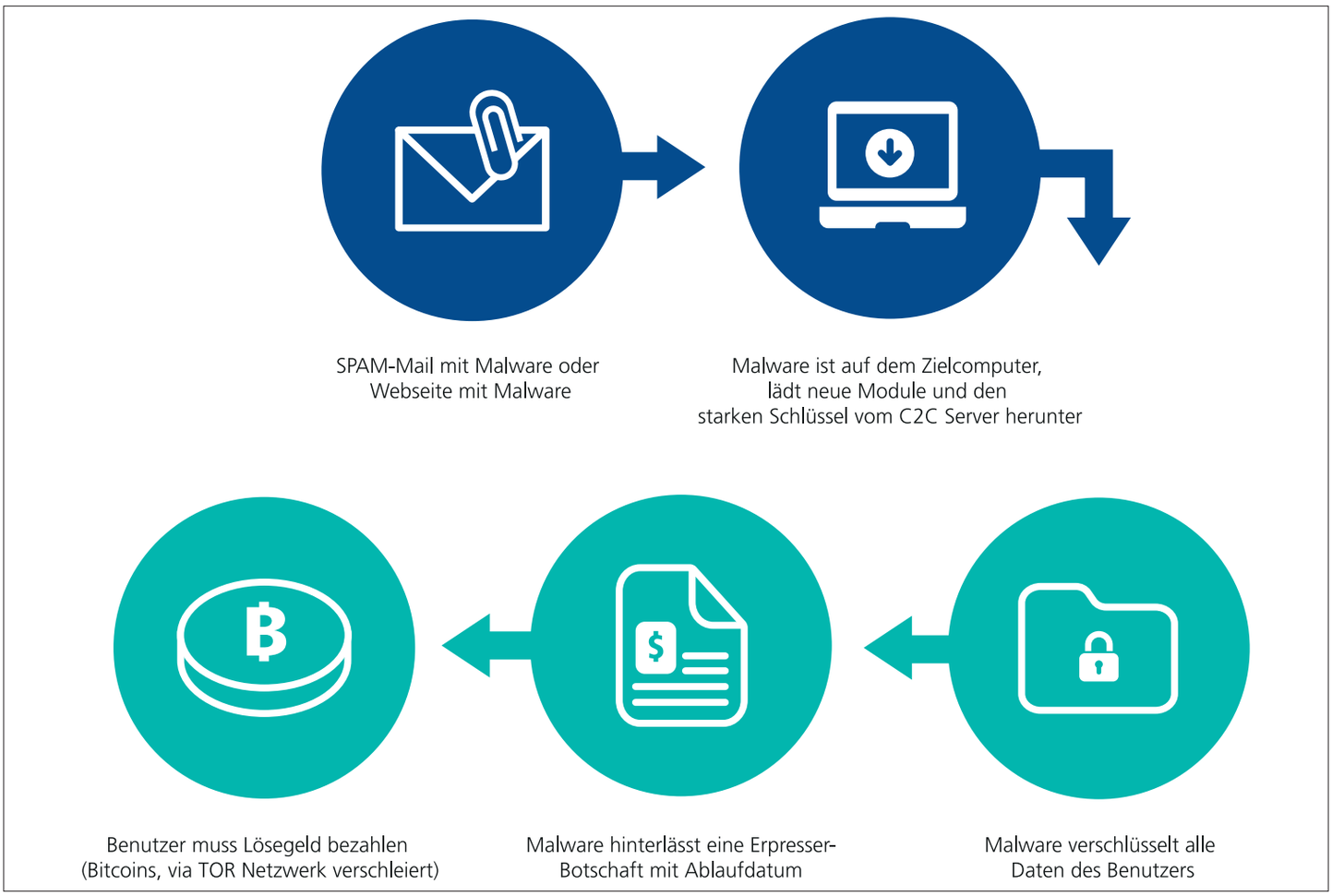
«Weil die Cryptoviren Dateien verschlüsseln», erklärt Urs Achermann. «Wenn z.B. ein KIS beim Starten oder Bearbeiten selber auf eine Datenablage zugreifen muss und diese gesuchten Dateien nicht vorhanden oder verschlüsselt sind, dann kann das System nicht weiterarbeiten. Der Datenzugriff ist unterbrochen.»

Das kann dramatisch sein, wenn ein Benutzer einen Cryptovirus eingefangen hat, und der gleiche Benutzer Zugriff und Schreibrechte auf ein internes Netzlaufwerk hat, auf welchem die Daten für das KIS abgespeichert sind:

1. Hier verschlüsselt der Virus zuerst alle lokal abgelegten Dateien.
2. Dann schaut er, worauf der infizierte Benutzer sonst noch Zugriff hat (und verlinkt ist).
3. So findet der Virus das verlinkte KIS-Netzlaufwerk und verschlüsselt dort alle wichtigen Daten.
4. Da die Applikation jeweils beim Systemstart wichtige Daten einlesen muss, diese aber gehackt sind, kann das KIS nicht mehr gestartet werden.

Auf diese Weise kann der Virusbefall bei einem einzigen Mitarbeiter ein KIS für die komplette Belegschaft ausser Betrieb setzen.

Werden «nur» Spitäler von diesen Viren angegriffen?



So läuft die unheilvolle Geschichte ab, wenn ein Hacker ins IT-System eingedrungen ist. Vorbeugen ist wirklich besser als Heilen.

«Mitnichten. Die Angriffe werden ziellos gestreut und können jeden treffen. Aufhorchen liess jedoch der Fall des Lukas Krankenhauses in Neuss. Als bekannt wurde, dass weitere Spitäler in Nordrhein- Westfalen betroffen waren und das Hollywood Presbyterian Medical Center ein Lösegeld von knapp 20000 US$ bezahlt hat, wurde klar, wie abhängig Institute des Gesundheitswesen von ihren IT-Systemen sind.

Ich habe in meiner Karriere in diversen IT-Bereichen gearbeitet. So kann ich vergleichen, wie die einzelnen Branchen in Bezug auf Sicherheitsmassnahmen und technische Hilfsmittel gegen Hacker gerüstet sind. Leider liegt das Gesundheitswesen 5 bis 10 Jahre hinter anderen Branchen (wie z.B. der Finanzindustrie) zurück. Das liegt auch daran, dass es oft am Bewusstsein für die Problematik fehlt. Möglicherweise hat der technologische Rückstand auch dazu beigetragen, dass gerade Spitäler angegriffen wurden.»

Kann es vorkommen, dass Cryptoviren trotz eines Antivirenprogramms aufs System gelangen?

«Leider ja. Die Autoren der Viren haben ihre Malware so geschickt programmiert, dass sich diese neuen IT-Krankheitskeime selber ständig verändern. So werden die neusten Mutationen eines Virus› von den herkömmlichen, signaturbasierten Antivirus-Herstellern nicht mehr erkannt.

Im ‹richtigen› Leben kann man sich das so vorstellen: Vor der Disco steht ein Bodyguard, der die bekannten Bösewichte vom Lokal fernhalten soll. Der Bodyguard weiss, dass ein Bösewicht ca. 40 Jahre ist, eine Brille und dazu eine Glatze mit Vollbart trägt. Genau diesen Bösewicht erkennt der Bodyguard und lässt ihn nicht ins Lokal. Wenn der Angreifer nun aber den Bart rasiert und die Brille durch Linsen ersetzt, dann wird er nicht mehr erkannt und gelangt problemlos ins Lokal.»

Gibt es gegen Cryptoviren keinen Schutz?

«Doch, aber das muss auf verschiedenen Stufen geschehen, organisatorisch wie technisch. – **Organisatorisch** ist Folgendes vorzukehren:

1. Trainieren und Sensibilisieren der Mitarbeiter heisst das zentrale Gegenmittel. Zeigen Sie ihren Mitarbeitenden auf, dass sich Attacken nicht nur in Hollywood ereignen, sondern auch hier bei uns drohen. Zeigen Sie Ihren Benutzern auf, dass sie nicht auf jeden Link klicken sollen, dass sie nicht jedes Attachment öffnen müssen, dass sie Ungewöhnliches sofort dem Service Desk melden und generell ihren ‹gesunden Menschenverstand› einsetzen dürfen.
2. Ebenso wichtig ist ein ‹Rollen- und Berechtigungskonzept› für den Schutz von Daten und Privatsphäre: Die Zugriffsrechte von Mitarbeitenden sollten so aussehen, dass sie alle Zugriffe bekommen, die sie für ihre Arbeit brauchen, aber nicht mehr.

Technisch sind folgende Massnahmen empfehlenswert:

1. Es ist wichtig, dass überall immer eine Antivirenprogramm läuft, welches die neusten Virensignaturen besitzt. Das hilft gegen alle bekannten Viren.
2. Weiter sollten die technischen Zugriffsrechte gemäss ‹Rollen- und Berechtigungskonzept›

restriktiv umgesetzt werden. Als Benutzer sollte man nicht mit Administrationsprivilegien arbeiten und auf keinen Fall mit Administrationsprivilegien im Internet surfen.
3. Und – ganz wichtig auch für alle Privatanwender: Immer ein aktuelles Backup der Daten erstellen!»

Gibt es professionelle Hilfe?

«Bei der HINT AG haben wir im Rahmen unserer ISO 27001 Zertifizierung ein ‹Security Operation Center› (SOC) aufgebaut. Davon profitieren unsere Kunden, die ihre IT-Dienste an uns ausgesourct haben. Unser Team arbeitet mit Überwachungstools, welche die Log- und System-Informationen vieler IT-Systeme in Echtzeit zentral sammelt und auswertet. So werden alle verdächtigen Internetzugriffe und ungewöhnliche Aktivitäten auf den Dateiservern analysiert. Mit dem SOC-Team haben wir im August 2015 den ersten Cryptovirus-Befall bei einem Kunden entdeckt. Wir suchten systematisch nach dem vom Virus befallene Benutzer. Als erste Sofortmassnahme musste der infizierte Computer vom internen Netz getrennt werden, so dass er keinen weiteren Schaden mehr anrichten konnte. Bei einem Vorfall wurden vom Cryptovirus innerhalb von 20 Minuten 20000 Dateien verschlüsselt, bei einem anderen Fall waren es über 140000 Dateien innerhalb von weniger als einer Stunde. Der einzige Weg, die Daten wieder brauchbar zu machen, ohne Lösegeld zu bezahlen, ist, das Backup der betroffenen Dateien wieder zurückzuspielen.

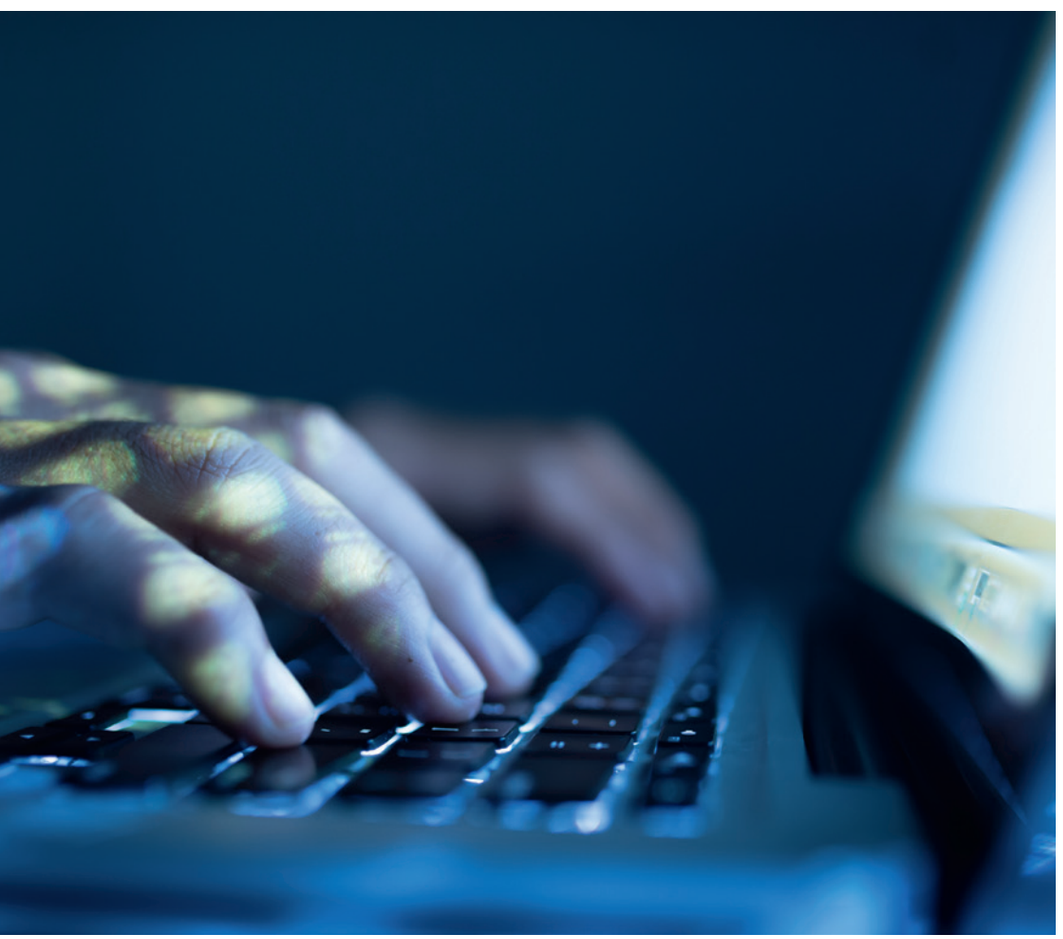
Aus diesen Vorfällen haben wir viel gelernt. Heute kann ich sagen, dass unser SOC-Team unglaublich schnell und professionell reagieren und so mögliche Schäden extrem reduzieren kann. Die Zeit, bis ein infiziertes System lokalisiert und isoliert wird, ist matchentscheidend. Ohne unser SOC hätte es an mehreren Orten zu längeren Ausfallzeiten wichtiger IT-Systeme kommen können.»

Kann ein Spital auch ein eigenes SOC aufbauen?

«Für ein eigenes SOC braucht es viel Know-how, Investitionen in die Infrastruktur und ausgebildete Mitarbeitende. Das kann man sich nicht überall selber leisten. Eine gute Alternative ist, seine IT-Infrastruktur von einem externen Spezialisten überwachen zu lassen, so dass Vorfälle sofort entdeckt und schnellstmöglich korrekte Gegenmassnahmen ergriffen werden können. Bevor man jedoch sicherheitskritische Aufgaben in Auftrag gibt, empfehlen wir, sich zuerst einen Überblick über die Situation im Unternehmen zu beschaffen. Zu beantworten sind folgende Fragen:
– Wie lange können Sie in Ihrem Betrieb auf die E-Mail Infrastruktur oder die interne Dateiablage verzichten?
– Sind Sie vorbereitet auf eine Hacker-Attacke?

Vielfach weiss das Management gar nicht, wo Lücken vorhanden sind. Die HINT AG bietet deshalb ein ‹Security Quick Assessment› an, das aufzeigt, wie eine Organisation bezüglich IT-Sicherheit nach ISO 27001 aktuell unterwegs ist. Das Assessment wird auf Interview-Basis durch erfahrene Sicherheitsexperten vor Ort durchgeführt.

Ziel des Assessments ist, aufzuzeigen, ob und wo Handlungsbedarf besteht. So können Zeit, Geld und Personal gezielt an den richtigen ‹Baustellen› (= roter Bereich) und nicht in bereits gut geschützte Domänen (= im grünen Bereich) investiert werden. Unsere Abbildungen zeigen die massgebenden Kriterien.»



Stichwort Arztgeheimnis. Dieses ist wohl auch in Gefahr …

«Ganz klar! Aktuell verschlüsseln Cryptoviren die Daten auf dem Zielsystem und verlangen Lösegeld. Am Beispiel des Hollywood Presbyterian Medical Center sieht man, dass dieses ‹Business-modell› funktioniert. Vielleicht gehen die Angreifer in einem nächsten Schritt weiter: Neben dem Verschlüsseln von Daten werden gleichzeitig Daten gestohlen. Nachdem man das erste Lösegeld erpresst hat, wird ein zweites gefordert: Entweder ihr bezahlt, oder ich mache die Krankenakte bekannter Persönlichkeiten öffentlich. Das wäre sowohl für die Betroffenen wie auch das Spital zur Katastrophe.

Schon bevor die ersten Schweizer Arztpraxen gehackt wurden, erschien im ‹Tagesanzeiger› ein Bericht, der exakt dies zum Thema gemacht hat: ‹Jeder zehnte Arzt verletzt die Schweigepflicht›. Unvorsichtigerweise werden heute Dienste wie Dropbox oder WhatsApp von Ärzten genutzt, um möglichst schnell von überall her auf Patientendaten zugreifen zu können. Dass diese Daten allerdings irgendwo in Amerika oder anderswo gespeichert werden, wo schlechte Datenschutzvorgaben existieren und die Integrität der Daten nicht garantiert ist, wird dabei oft ‹vergessen›.»

Immer mehr Patientendaten werden digital gespeichert? Wie sicher sind sie in einer Arztpraxis?

«Hier besteht ein virulentes Gefahrenpotenzial. Häufig sind gemäss Umfrage des ‹Tagesanzeigers› alle Patientendaten auf einer Festplatte gespeichert, auf die alle Praxismitarbeiter oder Kollegen einer Gemeinschaftspraxis Zugang haben. Ein Passwort ist die einzige Zugangsbarriere. Und der Server hängt am Netz. Da könnte ein Hacker zugreifen. 82 Prozent der Ärztinnen und Ärzte in der Schweiz speichern ihre Patientendaten laut Umfrage von Tagesanzeiger.ch/Newsnet, an der 256 Ärzte teilgenommen haben, lokal – also praxisintern. In fast der Hälfte der Arztpraxen haben sämtliche Mitarbeiter Zugang zum Computer, bei weiteren 32 Prozent sind es ausgewählte Mitarbeiter. Nur gerade 16 Prozent der Ärzte sagen, dass sie alleine Zugang zu den sensiblen Daten haben.

Die Bedrohung für das Berufsgeheimnis kann aber sogar vom berechtigten Anwender ausgehen: Eine kurze E-Mail-Anfrage mit Daten, die via Copy/Paste samt Patientennamen eingefügt werden, eine zu ausführliche Datei als Beilage, eine Röntgenaufnahme via WhatsApp, eine grössere Datei über Dropbox usw. Was auch immer ungeschützt bzw. unverschlüsselt elektronisch übermittelt wird, muss den Vergleich mit der Postkarte aus den Ferien nicht scheuen: Solange die Postkarte unterwegs ist, kann sie von jedermann gelesen werden. Während jedoch die Postkarte einem einigermassen direkten resp. vorgegebenen Weg zwischen Absender und Empfänger folgt, wird die elektronische Mitteilung hingegen von einem unbekannten Server zum nächsten weitgereicht und kann durchaus alle fünf Kontinente besucht haben, bevor sie den Empfänger erreicht. Die Frage, ob das Berufsgeheimnis dadurch nur bedroht oder verletzt wurde, erübrigt sich.»

Die Vernetzung in der Medizin schreitet munter voran? Werden wir immer unsicherer?

«Heute will man alles digital vernetzen. Das bietet enorme Vorteile. Wenn ein Herzschrittmacher autonom meldet, dass etwas nicht mehr stimmt, kann es lebensrettend sein. Aber genau diese Vernetzung macht das Gerät auch angreifbar.

Es ist denkbar, dass man einen Patienten mit üblen Absichten quasi virtuell entführen kann, dass man ihn erpresst und ihm androht, beim Herzschrittmacher die Frequenzen zu verändern.

Vernetzung birgt ein grosses Gefahrenpotenzial, nicht nur in der Medizin. Denken Sie nur an die selbststeuernden Autos – auch da liesse sich Gas- oder Bremspedal plötzlich von aussen steuern.»

Die Vernetzung verschiedener Akteure im Gesundheitswesen wird weiter zunehmen. Gleichzeitig wird sich der Datenaustausch deutlich intensivieren. Treiber dafür sind die stark wachsende Datenmenge immer raffinierterer bildgebender Verfahren und die verstärkte interdisziplinäre Zusammenarbeit der Leistungserbringer. Weiter ist auch das elektronische Patientendossier zu nennen, für dessen Einführung verschiedene Kantone mit ihren Communities schon wertvolle Vorarbeit geleistet haben. Mehr Vernetzung und Datenaustausch zeigen, wie entscheidend wirksame Massnahmen zur Datensicherheit und damit auch zur Integrität von Patienten und Versicherten sind. Die Spezialisten der HINT AG beraten Institutionen des Gesundheitswesens individuell und praxisnah.

Text: Dr. Hans Balmer