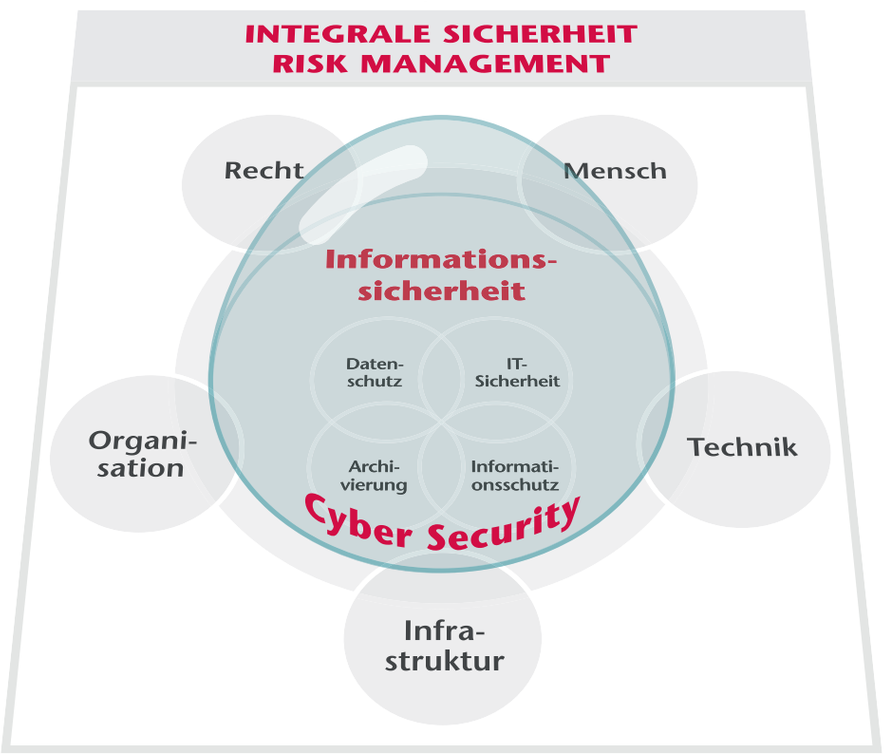
Auch nach dem britischen Beinahe-Kollaps: Nicht alle Spitäler kennen systematische Sicherheitskonzepte

Sicherheit hat viele Gesichter und ist eine Daueraufgabe

Mitte Mai haben breit angelegte Hacker-Attacken weite Teile des britischen National Health Services (NHS) in arge Bedrängnis gebracht. Mehrere Spitäler mussten ihre Tätigkeit für einen längeren Zeitraum teilweise einstellen. Ungenügend gesicherte IT-Systeme, veraltete Betriebssysteme und nicht befolgte Warnungen stellten Freipässe für Hacker dar. «Und es gibt noch weit mehr Gefahren, die ähnlich gravierend sein können», stellt Reto Zbinden, CEO der Swiss Infosec AG, fest.

«Ereignisse, die ein Spital lahmlegen könnten, sind immer schlimm», sagt der Sicherheitsexperte. «Cyber-Attacken gehören zu den bedrohlichsten. Es wäre allerdings ebenso gefährlich, sie als einzige Sicherheitsgefährdung anzusehen. Wir unterscheiden in unserer Beratungstätigkeit diverse Aspekte. – Grundsätzlich ist die integrale Sicherheit zu nennen, die es zu schützen gilt. Dazu gehören die physische Sicherheit im Rahmen von Zutrittsrechten, Brandschutz und auch der Schutz vor körperlichen Übergriffen. Weiter geht es um die medizinische Sicherheit, die u.a. die Behandlungssicherheit der Patienten und die Hygiene umfasst und um die Informationssicherheit. Diese beinhaltet die Elemente Datenschutz, Patientengeheimnis, IT-Sicherheit und Archivierung. Schliesslich sind auch Business Continuity und Krisenmanagement entscheidende Faktoren. Sie tragen dazu bei, die wichtigsten Betriebsprozesse aufrechtzuerhalten oder wiederherzustellen, sollten bereits schädliche Ereignisse eingetreten sein, die den Betrieb beeinträchtigen könnten. Sicherheit hat viele Facetten, die immer als Ganzes betrachtet werden sollten.»

Umfassende Sicherheit hat viele Gesichter. Die wichtigsten Einflussfaktoren, die es zu berücksichtigen gilt, sind Recht, Mensch, Technik, Infrastruktur und Organisation.



Ein grosses Thema – viel Nachholbedarf

Die Vielfalt der Gefahren ist eindrücklich und die Auswirkungen auf der Insel haben gezeigt, wie vernachlässigt offenbar gerade das Gesundheitswesen ist. «Dem ist so», pflichtet Reto Zbinden bei, «und wir stellen bei unserer Arbeit fest, dass auch in der Schweiz bezüglich des Schutzes vor sämtlichen genannten Gefahren ein grosser Nachholbedarf besteht. Positiv ist allerdings anzumerken, dass gewisse Spitäler schon vor einiger Zeit begonnen haben, sich intensiv mit der Thematik zu beschäftigen. Der Ernst der Lage ist seit Längerem bekannt, nur hapert es mit der Umsetzung entsprechender Gegenmassnahmen. Auch stellen wir fest, dass die Qualität der Umsetzung und laufenden Massnahmenoptimierung nicht überall der Best Practice entspricht bzw. mit dem nötigen Nachdruck erfolgt.»

Wo liegen denn die grössten Gefahren? – Reto Zbinden ist überzeugt, dass die Angriffe auf die NHS und ähnliche Vorfälle wie in Nordrhein-Westfalen und in Zürcher Arztpraxen zunehmen könnten, weil «ganz klar eine grosse Versuchung darin besteht, illegal an Patientendaten zu gelangen, die einen Geldwert haben und dazu dienen können, Spitäler zu erpressen oder durch Veröffentlichung sensitiver Daten Menschen direkt zu schaden. In die gleiche Richtung zielt eingeschleuste Ransomware, um damit den internen Zugriff auf behandlungsrelevante Daten zu unterbinden und den Betrieb des Hauses lahmzulegen. Man stelle sich vor: Bildgebende Verfahren gibt es nicht mehr, Operationen werden medizintechnisch nicht unterstützt, der restliche

Reto Zbinden, CEO Swiss Infosec AG

Minimalbetrieb muss wieder auf Papierbasis ablaufen. – Eine Katastrophe, die enorme Überbrückungskosten und materielle Schäden verursachen kann, juristische Konsequenzen wie z.B. Schadenersatzklagen nach sich ziehen könnte oder die Reputation eines Spitals für lange Zeit ruinieren kann!»

Wo ist primär anzusetzen?

Für unseren Interviewpartner ist es daher ausserordentlich wichtig, dass in einem Spital sichergestellt wird, dass die richtigen Menschen rechtzeitig die richtigen Massnahmen umsetzen. Am Anfang sieht er daher ein klares Regulativ, worin festgehalten wird, wer was im Rahmen der Sicherheit tun darf und damit sind zeitgemässe Weisungen mit eindeutiger Zuordnung von Verantwortlichkeiten und Entscheidungsbefugnissen erforderlich. «Vorhanden sind meistens relativ gute Dokumente, welche die Notwendigkeit beschreiben, was allerdings nicht genügt», erklärt Reto Zbinden. «Nehmen wir als Beispiel den Datenschutz: Hier handelt es sich um ein enorm hohes Gut, das auch mit Vertrauen in eine Institution verbunden ist. Hier ist nicht allein die Technik, etwa bessere IT-Systeme mit Firewalls und Authorisierungsregeln, entscheidend, sondern die kontinuierliche Überwachung der Informationsbearbeitung in all ihren Facetten. Gerade im Gesundheitswesen, das sich in einer ständigen Weiterentwicklung befindet und ein unerhört rasches Datenwachstum verkraften muss, heisst Stehenbleiben Rückschritt. Der Anschluss ist rasch verpasst, entsprechend lauern ebenso rasch wieder wachsende Gefahren.»

Gleiches gilt für die regelmässige Information und Ausbildung der Mitarbeitenden aller Stufen: Bewusstsein schaffen, Gefahrenpotenzial orten, spezielle Situationen trainieren und damit ein umfassendes Sicherheitsdenken fördern.

Ohne Organisation geht's nicht

Es gehe um eine integrale Sicherheit und dazu bedürfe es einer wirkungsvollen Organisation. Im Zentrum stehe ein/e Sicherheitsdelegierte/r. Bei dieser Fachperson, die über eine grosse technische Kompetenz wie auch Verständnis für wirtschaftliche Zusammenhänge und Kommunikation verfügen muss, laufen die Fäden zusammen. In den einzelnen Bereichen wirken Sicherheitsbeauftragte, die sich regelmässig mit dem/der Beauftragten zum Erfahrungsaustausch treffen. So entstehen nebst Verständnis und Transparenz rasch die gewünschten Synergieeffekte.

Es entsteht auch Beratungsbedarf. «Wir stellen seit einiger Zeit fest, dass die Nachfrage nach gezielter Beratung zunimmt», berichtet Reto Zbinden. «Wir bauen dabei eine starke Spitalorganisation auf, wir unterstützen den/die Sicherheitsdelegierte/n, analysieren die Gefahren und betrieblichen Abläufe, wir optimieren das Sicherheitsszenario und begleiten parallel dazu die verantwortlichen Stellen für Technik und IT. In vielen Fällen sind wir nach der Initialphase in der Regel quartalsweise vor Ort und diskutieren mit dem/der Delegierten und den Sicherheitsbeauftragten alle relevanten Erkenntnisse. In der Zwischenzeit kümmern sich diese Fachleute um das Tagesgeschäft und die operationellen Sicherheitsrisiken. Einmal im Jahr findet schliesslich eine gründliche Review im Rahmen des Internen Kontrollsystems (IKS) statt, die wir mitgestalten. Dabei geht es nicht nur um den Finanzbereich, sondern auch um die Überprüfung der IT-Infrastruktur, beispielsweise der Firewalls, Benutzerrechte und andere relevante datentechnische Aspekte.»

Kapazitätsengpässe schaffen auch Risiken

Gerade weil die Gefahren, die lauern, enorm sind, darf nichts dem Zufall überlassen werden. Wenn nun aber personelle Engpässe bestehen, kann hier neues Gefahrenpotenzial entstehen. Womit wir wieder bei der IT sind. «Es ist offensichtlich, dass die Spital-IT-Abteilungen oft nicht über genügend Personal verfügen, um neben den grossen Anforderungen der Geschäftsleitung im Rahmen von Infrastruktur und Applikationen auch noch prophylaktisch für eine kompromisslos hohe Sicherheit zu sorgen. Es kann auch vorkommen, dass die Meinung besteht, nur mit Investitionen sei bereits für eine erstklassige IT-Architektur gesorgt. Das ist ein Trugschluss. Zu sichern sind auch die Prozesse und Ressourcen, ebenso die Kompetenzen und das Gefahrenbewusstsein der IT-Fachleute.

Lücken werden oft sichtbar, wenn neue Systeme – etwa ein KIS – evaluiert und eingeführt werden. «Generell können wir sagen», so Zbinden, «dass das rasante Datenwachstum, die Digitalisierung und Vernetzung verschiedener Akteure im Rahmen der integrierten Versorgung einen enormen Druck auslösen. Die Verantwortlichen bei Management, Technik, Betrieb und IT werden sich aber der Gefahren immer deutlicher bewusst. Schliesslich möchte ein Spital auch nicht Zeit vergeuden, um mit dem kantonalen Datenschutzbeauftragten die Klingen zu kreuzen, wenn Unzulänglichkeiten zu Tage treten. Rechtzeitig gezielt vorzubeugen, ist auf alle Fälle ein gutes Rezept.»

Was wenn schon etwas passiert ist?

Neben IT- und Datenschutzproblemen sind auch mannigfache technische Gefahren zu beachten. So kann ein Stromunterbruch erfolgen oder ein Problem mit der Sauerstoffversorgung auftauchen. Das interne Sicherheitsteam beugt hier mit der Schaffung nötiger Redundanzen vor, verbessert die Abläufe und installiert eine bessere Infrastruktur, etwa Generatoren, dezentrale Sauerstofftanks, unterbrechungsfreie Stromversorgung, Datenspiegelungen, externe Archivierungen und anderes mehr.

All das sorgt für eine ausreichende Business Continuity. «Damit verbunden ist meist auch ein Krisenmanagement», betont der Sicherheitsexperte. «Auch das muss erstklassig organisiert sein, mit Analysen, Konzepten und Verantwortlichkeiten. Analog militärischer Vorgehensweisen müssen der Führungskreislauf, der Prozess für Lageanalysen bei existierenden Vorfällen und das Treffen von Sofortmassnahmen unmissverständlich vorgängig festgelegt sein. Es wäre falsch anzunehmen, dass die Geschäftsleitung aus dem Stand heraus in der Lage wäre, solche Fälle zu lösen, dies auch weil es Extremfälle gibt, die über mehrere Tage andauern können. Auch hier bieten wir unsere Unterstützung an.»

«Sicherheit beginnt zuoberst, in der Geschäftsleitung. Sicherheit muss alle Bereiche und Stufen des Unternehmens erfassen. Es geht um Analysen, Konzepte, Richtlinien, Weisungen und kompetent besetzte Stellen», fasst Reto Zbinden zusammen, «kein Detail darf vernachlässigt werden, denn es geht im Spital im wahrsten Sinne des Wortes um Leben und um die weitestmögliche Wahrung der Integrität der Patienten.»

Interview: Dr. Hans Balmer