IT-Sicherheit stärker in den Fokus rücken

Die Cybersicherheit rückt immer weiter in den Fokus. Bundesinnenministerin Nancy Faeser will zum Schutz vor Cyberattacken sogar die Kompetenzen des Bundes ausbauen und das Grundgesetz ändern. Im Gespräch erläutern Michaela Grundmeier und Thomas Althammer, wie Pflegeeinrichtungen ihre Daten und IT-Systeme schützen können.

Interview: Ina Füllkrug

Betrifft das Thema Sicherheit von Daten und IT-Systemen auch die Gesundheits- und Sozialwirtschaft, kleine und mittelständische Organisationen?

Michaela Grundmeier: Die fortschreitende Digitalisierung – auch und besonders in der Pflege – sorgt für steigende Risiken, Opfer einer Cyberattacke zu werden. Denn dort locken großen Mengen besonders sensibler Patientendaten und damit ein hohes Erpressungspotenzial, wenn Daten nicht mehr verfügbar sind. Wer glaubt, dass kleine Pflegeorganisationen doch bestimmt kein hohes Risiko haben, der irrt. Gerade kleine und mittelständische Organisationen sind wenig geschützt und damit attraktive Angriffsziele. Frau Faeser bezieht sich vor allem auf Organisationen der kritischen Infrastruktur, aber auch alle anderen Akteure müssen Cybersicherheit künftig viel mehr im Fokus haben als bisher.

Auf welchen Wegen können Angreifer in IT-Systeme eindringen und inwiefern öffnet der Mensch, der die Systeme nutzt, unbeabsichtigt Türen?

Thomas Althammer: Grob gesagt gelangen Angreifer auf zwei Wegen in IT-Systeme. Entweder verschaffen sie sich Zutritt über eine Sicherheitslücke oder Konfigurationsfehler im System oder der Angriff erfolgt über den Menschen, der das IT-System bedient. Für beide Möglichkeiten existieren eine Vielzahl an Optionen, sogenannte Angriffsvektoren, die sich genauso schnell weiterentwickeln, wie neue Systeme und Sicherheitsstandards entstehen. Dementsprechend ist es sinnlos, einmalig in die Sicherheit der eigenen Systeme zu investieren. Es handelt sich vielmehr um einen laufenden Prozess der regelmäßigen Anpassung und Optimierung. Das Vorgehen der Cyberkriminellen hat sich dabei im Laufe der Jahre immer weiter professionalisiert. Heute beginnt ein Angriff mit umfangreichem Ausspionieren des Opfers, dem Sammeln von Informationen und dem Austesten der IT-Systeme. Wurden Lücken identifiziert, wird die Attacke dezidiert geplant und umgesetzt. Dieser Prozess kann sich über mehrere Monate erstrecken.

Was sind die bekanntesten Schwachstellen, die Angreifer nutzen?

Althammer: Cyberkriminelle nutzen aus, dass bereits bekannte Sicherheitslücken in Systemen nicht rechtzeitig geschlossen werden. IT-Systeme, die nicht auf dem neuesten Stand der IT-Sicherheit sind, etwa durch unregelmäßiges Updaten der Systeme, bieten ebenso Möglichkeiten des Eindringens. Auch sogenannte Schatten-IT, die z. B. von Mitarbeitenden ohne Kenntnis der IT-Verantwortlichen installiert wurde, kann ein Einfallstor sein. In den vergangenen Jahren haben sich Phishing-Mails zu einer der beliebtesten Methoden entwickelt, um in IT-Systeme einzudringen und Schadsoftware zu implementieren. Der Boden für eine erfolgreiche Cyberattacke wird von den Organisationen oft selbst bereitet. Wir sehen, dass Verantwortlichkeiten nicht klar definiert sind und Sicherheitskonzepte sowie Maßnahmen fehlen, um die eigenen Daten und die Systeme sinnvoll zu schützen.

Worauf müssen sich Pflegeeinrichtungen in Sachen Cyberkriminalität einstellen? Wie können sie ihre Daten und IT-Systeme schützen?

Grundmeier: Die Digitalisierung ist nicht aufzuhalten. Die Branche muss sich darauf einstellen, dass die Frage nicht mehr lautet, ob man Opfer einer Cyberattacke wird, sondern wann (oder bereits schon wurde). Ein Augenmerk sollte auf der Schadensbegrenzung liegen, z. B. durch Segmentierung von Netzwerken und das Einziehen von Schranken hinter der Firewall. Wir sehen seit Jahren stark steigende Zahlen von Cyber-Attacken auf Unternehmen und Organisationen. Man muss sich klar machen, dass bis zu 553 000 neue Schadprogramm-Varianten entstehen – pro Tag wohlgemerkt. Diese Zahl stammt vom Bundesamt für Sicherheit in der Informationstechnik. Und das Bild ändert sich kontinuierlich. Noch vor wenigen Jahren war Phishing kaum ein Problem, heute sind die Mails so geschickt getarnt, dass selbst IT-Verantwortliche Schwierigkeiten haben können, diese zu identifizieren.

Doch was heißt das für die Pflege-Unternehmen? Das Management müsste die IT-Sicherheit mehr in den Fokus nehmen und Budgets dafür einplanen. Und die Mitarbeitenden sollten regelmäßig geschult und für die Bedrohungslagen sensibilisiert werden. Dann wäre schon viel gewonnen.

Foto: Althammer & Kill

Thomas Althammer, Datenschutzbeauftragter in der Altenpflege und Geschäftsführer, Althammer & Kill, Hannover.

Foto: Caritas

Michaela Grundmeier, betriebliche Datenschutzbeauftragte/Projektentwicklung, Caritas Seniorenheime GmbH, Warendorf.

Wo können kleine und mittelständische Einrichtungen ansetzen, die keine großen Budgets zur Verfügung haben und keine IT-Abteilung?

Grundmeier: Auseinandersetzung steht am Anfang – ganz unabhängig von Budgets. Machen Sie eine Bestandsaufnahme und stellen Sie fest, welche Systeme wie genutzt werden. Legen Sie fest, welchen Schutzbedarf jedes System hat und identifizieren Sie die „Kronjuwelen", die unbedingt geschützt werden müssen. Welche Personen haben welche Berechtigungen – und sind alle Nutzer geschult im Umgang mit IT sowie sensibilisiert für die Risiken? Als nächstes sollte man sich fragen, welche Anwendungen überhaupt Zugang zum Internet brauchen, welche Seiten im World-Wide-Web von Nutzern benötigt werden und welche Inhalte blockiert werden sollten. Welche Schutzmaßnahmen gibt es für die Netzwerke und Systeme: Firewalls, Mailfilter, Antivirenprogramme und wie sind diese konfiguriert? Werden wichtige Daten regelmäßig gesichert? In der Auseinandersetzung mit der Cybersicherheit können schon viele Risiken mit wenig Aufwand minimiert werden. Der Lagebericht von Finsoz stellt acht Handlungsoptionen sehr ausführlich dar und gibt einen guten Überblick. Und zuletzt sind kleine Budgets sehr viel besser, als keine Budgets – man muss sie nur clever einsetzen.

Was ist im Fall der Fälle zu tun, wenn eine Cyberattacke erfolgreich war?

Althammer: Das hängt maßgeblich von der Art des Angriffs und dem Ausmaß des Schadens ab. Oftmals werden Attacken erst spät bemerkt. Durchschnittlich dauert es 207 Tage, bis ein Angriff entdeckt wird und in dieser Zeit kann viel Schaden entstehen. Sind „nur" einzelne Systeme betroffen, müssen diese zügig isoliert werden. Der Angriff auf ein Unternehmen aus dem Diakoniebereich konnte nur ohne Lösegeldzahlung abgewendet werden, weil funktionierende Backups vorlagen, Netzwerke isoliert werden und parallel in neuer Struktur wieder aufgebaut werden konnten. Gibt es wenig IT-Expertise in der eigenen Organisation kann es ratsam sein, sich schnell Unterstützung durch externe Profis zu holen. Diese beschäftigen sich auch eingehend mit der „Digitalen Forensik". Dabei geht es darum, den Angriff zu rekonstruieren und nachzuvollziehen, wie ein Angreifender in die Systeme gelangt ist, auf welche Anwendungen er Zugriff hatte und wo potenziell Schadcodes liegen könnten, um diese zu eliminieren und Lücken zu schließen.

Ist der Anschluss an die TI ein Weg, um mit wenig Aufwand Datenschutz und IT-Sicherheit zu steigern?

Grundmeier und Althammer: Der Anschluss an die Telematikinfrastruktur (TI) bedeutet die Vernetzung aller im Gesundheitswesen beteiligten Akteure, um Informationen des Versicherten auf einem einheitlichen standarisierten Weg elektronisch zur Verfügung zu stellen. Die „Spielregeln" werden u. a. von der gematik GmbH vorgegeben. Aber auch „Spielregeln" müssen eingehalten werden. Um diese Gesundheitsplattform nutzen zu können, müssen alle Akteure natürlich auch ein Verständnis von IT-Sicherheit haben. Bei der Installation der Konnektoren an die eigene Infrastruktur gilt es beispielsweise zu verstehen, welche Ports freigeschaltet werden müssen und was dies für die Unternehmens-IT bedeutet. Der Aufwand für den Datenschutz und die IT- Sicherheit wird sicherlich nicht geringer. Aber Faxen und der Versand von unverschlüsselten Mails, um Gesundheitsdaten von A nach B zu bekommen, sind keine Alternative.

MEHR ZUM THEMA

Info: www.althammer-kill.de; www.finsoz.de