IT-Sicherheit ist Chefsache

Schweizer KMU sind beliebte Ziele von Cyberkriminellen. Auch Arztpraxen können ins Visier geraten. Worauf Ärzte achten sollten, erklärt Pascal Lamia, Leiter von Melani, der Melde- und Analysestelle Informationssicherung des Bundes.

Interview: Markus Gubler, Presse- und Informationsdienst
Bilder: Béatrice Devènes

Pascal Lamia: «Cyberkriminelle setzen auf die bewusste Irreführung und missbrauchen dazu vor allem bekannte und vertrauenswürdige Firmen in der Schweiz: Swisscom, Steuerverwaltung, Migros, Coop.»

Pascal Lamia, wie sieht ein gewöhnlicher Arbeitstag des Leiters der Melde- und Analysestelle Informationssicherung Melani aus?
Gewöhnliche Arbeitstage gibt es nicht. Ich bin ein Frühaufsteher und komme gegen 6.30 Uhr ins Büro. Zu dieser Zeit kann ich mir in aller Ruhe einen Überblick verschaffen: Wie sieht die aktuelle Bedrohungslage aus? Welche Meldungen kamen über Nacht rein? Wo stehen die Fälle, die wir in den vergangenen Tagen bearbeitet haben? Über das Meldeformular auf unserer Website können uns Privatpersonen wie KMU verdächtige Vorfälle melden. Jährlich erreichen uns rund 10000 Meldungen.

Welchen Auftrag hat Melani?
Unser Grundauftrag lautet, die kritischen Infrastrukturen in der Schweiz zu schützen. Dazu zählen beispielsweise Energieversorgung, Pharma- und Chemieindustrie, Telekommunikation, Finanz- und Versicherungswesen, aber auch die öffentliche Verwaltung sowie das Rettungs- und Gesundheitswesen. Wir beobachten und analysieren die aktuelle Lage, um möglichst früh vor Bedrohungen zu warnen. Dazu stehen wir in engem Kontakt mit Betreibern kritischer Infrastrukturen und unterstützen sie beim Bewältigen von Vorfällen. Der Bundesrat formulierte unseren Auftrag im Jahr 2003. Er hat den Handlungsbedarf in der Cyberabwehr somit früh erkannt. Bislang erstreckt sich unser Auftrag nicht auf KMU oder private Personen. Mit der neuen Cyberstrategie will man dies ändern. Künftig sollen auch KMU unsere Dienste nutzen können. Dafür müssen wir personell aufrüsten. Die aktuell 19 Beschäftigten von Melani reichen nicht aus.

Wie sehen Cyberattacken gegenwärtig aus?
Die Schweiz war und ist für Angreifer ein attraktives Ziel. Die Schweiz ist ein kleines, modernes, innovatives Land. Wir haben sehr gute Internetanbindungen, viele Haushalte sind vernetzt. Unzählige erledigen ihre Geldangelegenheiten per E-Banking. Und wir haben viele kleinere und mittlere Unternehmen, welche durchaus interessante Informationen für Cyberangriffe haben.

Folgen die Attacken einem bestimmten Muster?
Ein Angreifer hat im Grunde zwei Möglichkeiten: Gewitter oder gezielter Angriff. Bei einem Gewitter überdeckt er die Schweiz mit einer Welle von Spammails. Zwischen Privatpersonen, KMU oder kritischer Infrastruktur wird nicht unterschieden.

Das Ziel ist: möglichst viele Geräte, möglichst viele Systeme zu infizieren. Bei gezielten Angriffen suchen sich die Angreifer bestimmte KMU aus, um sie beispielsweise gezielt mit Verschlüsselungstrojanern zu verseuchen oder um an wichtige Informationen zu gelangen. Die betroffenen KMU sehen sich dann beispielsweise mit Lösegeldforderungen konfrontiert, die schnell 10000 Franken übersteigen oder merken viel zu spät, dass ihnen Informationen gestohlen worden sind.

Damit ein Angreifer in ein Netzwerk eines KMU eindringen kann, muss die Türe von innen geöffnet werden. Richtig?

Ganz genau. Es braucht den menschlichen Faktor. Angestellte in KMU oder Mitarbeitende in Arztpraxen müssen infizierte Links oder angehängte Dateien in Mails manuell anwählen, damit die schädliche Software aktiviert wird. Es ist aber auch schon vorgekommen, dass Mitarbeitende Spammails in privaten Mailkonten angeklickt haben und sich die Spionagesoftware erst durch das Einloggen ins Firmennetzwerk ausbreitete.

Cyberkriminelle setzen auf die bewusste Irreführung …

… und missbrauchen dazu vor allem bekannte und vertrauenswürdige Firmen in der Schweiz: Swisscom, Steuerverwaltung, Migros, Coop. Die schädlichen E-Mails werden mittlerweile so gut nachgebaut, dass sie sich kaum mehr von echten unterscheiden. Digitale Signaturen und Verschlüsselungen würden die Sicherheit erhöhen. Sie flächendeckend einzusetzen ist aber enorm aufwändig.

Wenn eine flächendeckende Einführung von digitalen Signaturen kaum realistisch ist, welche Alternativen haben KMU und Privatpersonen, um sich vor Cyberangriffen zu schützen?

Wir empfehlen vorausschauend zu handeln. Firmenbesitzer wie Praxisinhaber sollen sich Gedanken über ihre IT machen. Wie organisiere ich den Betrieb, wenn meine IT nicht funktioniert? Kann ich ohne IT überhaupt arbeiten? Weiter: Bin ich selber für die IT zuständig oder ziehe ich Dritte bei? Bei Letzterem muss ich sicher sein, dass mein IT-Partner die Datensicherung im Griff hat. Kann er bei einer Datenverschlüsselung rasch die Daten des gestrigen Tages zurückspielen und das System so wieder in Gang setzen? Jeder Unternehmer muss sich solche Fragen individuell stellen.

Offenbar hat sich diese Einsicht noch nicht überall durchgesetzt, sonst hätten Sie wohl den Cybersecurity-Schnelltest für KMU nicht kürzlich vorgestellt.

Richtig. Melani hat aber den Schnelltest nicht entwickelt, sondern nur inhaltlich begleitet. ICT Switzerland und weitere Organisationen haben das Projekt vorangetrieben. Wir wollten den KMU nicht ein 200-seitiges Regelwerk mit Empfehlungen vorlegen. Dies wäre nicht stufengerecht. Der Schnelltest besteht aus einem Fragebogen, der in fünf bis zehn Minuten ausgefüllt werden kann. Anhand der eigenen Antworten sehen die einzelnen KMU, wo sie in punkto IT-Sicherheit stehen. Der Schnelltest soll eine Entscheidungshilfe sein.

Der Schnelltest ist also auch eine Sensibilisierungskampagne.

Definitiv. Wir haben viele KMU, die sich an uns gewandt haben, nachdem sie angegriffen wurden. Und die erste Frage, die immer gestellt wurde: Wie hätte ich die Attacke verhindern können? Der Schnelltest soll dazu beitragen, sich mit der Problematik von Cyberangriffen auseinanderzusetzen.

Worauf soll ein Arzt in seiner Praxis besonders achten?

Viele Geräte, gerade die neueren, verfügen über einen eigenen Internetanschluss. Damit können die Hersteller direkt auf die Geräte zugreifen, um die Software zu aktualisieren und die Leistungsdaten abzurufen. Dessen muss sich der Arzt oder der Praxisinhaber bewusst sein. Er soll sich bei den Herstellern nach deren Sicherheitsstandards erkundigen. Denn: IT-Sicherheit ist immer Chefsache. In meinen Augen ist das Auslagern der IT ab einer gewissen Unternehmensgrösse aber sinnvoll.

Um die IT-Sicherheit zu überprüfen, wurde ein Schnelltest für KMU entwickelt. Der Fragebogen kann online in wenigen Minuten ausgefüllt werden.

Sollen Praxen eigene Lösungen aufbauen oder könnte auch ein Berufsverband Standards empfehlen?

Ein interessanter Gedanke. Es existieren heute ja bereits Anbieter wie HIN, die E-Mail-Verschlüsselungen und Software-Support in diesem Bereich anbieten. Ob sich flächendeckende Lösungen durchsetzen, ist letztlich eine Preisfrage. Ein Verbandsmitglied, das nicht mehrere Tausend Franken jährlich in seine IT investieren will, wird sich einer standardisierten Lösung anschliessen. Auch wenn sich keine Standards durchsetzen lassen sollten, so kann der Berufsverband aber seine Mitglieder regelmässig für die Themen IT-Sicherheit und Cyberkriminalität sensibilisieren.

Dieser Artikel erschien erstmals im Swiss Dental Journal SSO 11/2018 und wird mit freundlicher Genehmigung der Fachzeitschrift nachgedruckt.

Tipps vom IT-Sicherheitsexperten

Sind die Daten extern verschlüsselt worden, lassen sie sich nur schwer oder gar nicht wiederherstellen. Mit den folgenden Massnahmen erhöhen Sie die IT-Sicherheit in Ihrer Arztpraxis.

1. Öffnen Sie E-Mails nicht unter Stress. Warten Sie auf einen ruhigeren Moment.
2. Überlegen Sie sich, ob Sie von dieser Firma eine Anfrage erwarten. Löschen Sie im Zweifelsfall die E-Mail!
3. Machen Sie von Ihren Daten tägliche Backups.
4. Speichern Sie die täglichen Backups auf verschiedenen externen Harddisks.
5. Lagern Sie die externen Harddisks an verschiedenen Standorten.
6. Arbeiten Sie mit Harddisks verschiedener Generationen.