«Die Angreifer schlafen nicht»

Kriminelle missbrauchen die Coronakrise für gross angelegte **Cyberangriffe auf KMU.** Davon sind auch Zahnarztpraxen betroffen. Was Praxisinhaber beachten sollten, weiss Pascal Lamia, Leiter der Operativen Cybersicherheit des Bundes und der Melde- und Analysestelle Informationssicherung MELANI.

Interview: Markus Gubler, Andrea Renggli, Redaktion SDJ
Foto: Béatrice Devènes, Fotografin

Pascal Lamia, in Krisenzeiten versuchen Kriminelle gezielt, Ängste und Sorgen der Bevölkerung auszunützen. Welche Aktivitäten haben Sie während des Lockdowns beobachtet?
Sehr oft werden aktuelle Geschehnisse für Angriffe missbraucht. Angreifer versuchen die Ängste und Sorgen der Bevölkerung für ihre Zwecke auszunutzen. So beobachtet das Nationale Zentrum für Cybersicherheit (NCSC) regelmässig bei Ereignissen wie Unwetterkatastrophen, Erdbeben usw. eine Zunahme von Cyberangriffen. Sehr beliebt sind beispielsweise betrügerische E-Mails, in denen die Angreifer sich auf das Ereignis beziehen und zu Spenden für die Betroffenen aufrufen. Die Coronakrise zeigte ein ähnliches Bild: Es gab hunderte von vermutlich betrügerischen Internetseiten mit .ch-Domain. Das NCSC hat ein Monitoring eingerichtet, um solche Seiten zu identifizieren. Jene Seiten, die sich als betrügerisch oder schadhaft erwiesen haben, liess das NCSC in enger Zusammenarbeit mit den zuständigen Partnern (Internet Service Provider, Switch usw.) sperren. Das NCSC bleibt in engem Kontakt mit diesen Partnern und hält das Monitoring vorderhand noch aufrecht. Im Bedarfsfall kann das NCSC somit sehr schnell reagieren.

Die Schweiz erlebte in den vergangenen Wochen einen Digitalisierungsschub. Die Infrastrukturen mussten teilweise sehr rasch aufgebaut werden, für Sicherheitsarchitektur blieb wenig Zeit. Welche Systeme müssen nachgerüstet werden?
Müssen in Krisenzeiten Infrastrukturen in kürzester Zeit aufgebaut werden, gilt es im Sinne des Business Continuity Managements immer abzuwägen zwischen Aufrechterhalten des Betriebs und Abdecken der Sicherheitsanforderungen. In jedem Fall muss spätestens am Ende einer Krise der Rückbau der Notfallinfrastruktur so rasch wie möglich angegangen werden, damit die Sicherheit der Systeme wieder hergestellt ist. Welche Systeme nachgerüstet werden müssen, hängt sehr stark von der vorhandenen Infrastruktur und vom Bereich ab, in dem ein Unternehmen tätig ist. Bei einer Zahnarztpraxis dürfte der Fokus bei Systemen mit Patientendaten liegen, die bestmöglich vor dem unbefugten Zugriff durch Dritte geschützt werden müssen. Bei einem Onlineshop hingegen ist die Verfügbarkeit des Shops von hoher Wichtigkeit, damit weiterhin Umsätze generiert werden können. Die Unternehmen sind jedoch nicht erst seit der Coronakrise für die Sicherheit der Daten und Informationen verantwortlich. Dies war bereits vorher der Fall und gilt selbstverständlich auch für die Zukunft. Cybersicherheit muss auf der Geschäftsleitungsebene verankert sein. Ist dieses Verständnis nicht vorhanden, ist der Schutz meistens nicht ausreichend.

Entstehen besondere Sicherheitsrisiken, wenn viele Angestellte im Homeoffice arbei-

Vorsicht vor gefälschten Rechnungen

Seit Kurzem verzeichnet das NCSC vermehrt Meldungen von Business E-Mail Compromise (BEC) oder Überweisungsbetrug. Das heisst, dass Betrüger in kompromittierten E-Mail-Kontos von Mitarbeitern oder in Konten einer Online-Kollaborationsplattform nach elektronischen Rechnungen suchen, diese mit einer anderen IBAN versehen und erneut zustellen. Immer häufiger nehmen Betrüger die Identität von externen Geschäftspartnern oder Subunternehmen an und schicken Rechnungen mit abgeänderter IBAN an deren Kunden, Partner oder Nebenstelle. Oftmals liefert die Kompromittierung einer Online-Datenaustauschplattform Kriminellen die notwendigen Informationen auf dem Silbertablett. Sie suchen zum Beispiel im Kalender nach Informationen, um eine passende Geschichte zu kreieren. Aber auch Betrugsversuche, bei denen sich der Angreifer als eine Person innerhalb des Zielunternehmens ausgibt, sind weiterhin üblich bis hin zu simplen Versuchen, gefälschte Rechnungen unterzujubeln oder in einem Schreiben vorzutäuschen, die Kontonummer habe geändert.

Massnahmen:
- Definieren Sie Prozesse und Sicherheitsmassnahmen und setzen Sie diese um. Sie können hierfür das NCSC-Merkblatt «Informationssicherheit für KMU» konsultieren (www.ncsc.admin.ch > Dokumentation > Checklisten und Anleitungen).
- Sensibilisieren Sie die Mitarbeitenden dahingehend, dass alle definierten Prozesse und Sicherheitsmassnahmen jederzeit einzuhalten sind.
- Insbesondere sollten alle Geldtransfers nach dem Vier-Augen-Prinzip mit Kollektivunterschriften erfolgen. Ankündigungen von Kontoänderungen ist besondere Aufmerksamkeit zu schenken.
- Aktivieren Sie auf Online-Kollaborationsplattformen die Zwei-Faktor-Authentisierung.

Pascal Lamia, Leiter Operative Cybersicherheit des Bundes: «Cybersicherheit muss auf der Geschäftsleitungsebene verankert sein. Ist dieses Verständnis nicht vorhanden, ist der Schutz meistens nicht ausreichend.»

ten? Welche ungesicherten oder zu wenig gesicherten Schnittstellen gibt es in Zahnarztpraxen?
Das NCSC beurteilt die Sicherheitsrisiken bei Homeoffice nicht anders als bei der Arbeit in der Praxis. Die Mitarbeitenden müssen sich ihrer Verantwortung im Umgang mit sensiblen Daten bewusst sein. Somit sollten Zahnarztpraxen ihren Angestellten genaue Vorgaben machen, wie sie richtig mit den Daten und Informationen umgehen müssen. Dies gilt auch, wenn die Hardware, unabhängig ob defekt oder veraltet, ersetzt wird: Was geschieht beispielsweise mit den Daten auf der Harddisk? Diese und andere Fragen müssen im Vorfeld geklärt und vorgegeben sein. Ein besonderes Augenmerk gilt aber sicher auch den Remote-Zugängen. Können der Arzt oder die Mitarbeitenden beispielsweise von zu Hause aus auf die Infrastruktur und Daten in der Praxis zugreifen, so muss dieser Zugriff speziell gesichert werden. Die Verbindung muss verschlüsselt und mittels einer Zwei-Faktor-Authentisierung, also User-ID, Passwort und einen zusätzlichen Faktor wie beispielsweise einer SMS, gesichert sein.

Viele Geräte in Zahnarztpraxen sind mit dem Internet verbunden. Sind die Hersteller in der aktuellen Lage besonders gefordert, die Sicherheit ihrer Geräte zu garantieren? Oder ist das Sache des Praxisinhabers?
Die Hersteller waren sich lange Zeit der Gefahren nicht oder zu wenig bewusst, was dazu führte, dass neue Geräte zwar gut und günstig waren, jedoch die Sicherheit vernachlässigt wurde. Unterdessen hat bei den Herstellern ein Umdenken stattgefunden und sie versuchen, von Anfang an eine möglichst gute Sicherheit in ihre Geräte zu implementieren. Die Verantwortung für die Sicherheit der IT liegt jedoch bei den Praxisinhaberinnen und -inhabern.

Im April 2020 hat die Global Cyber Alliance (GCA) zusammen mit ICTswitzerland und der Schweizerischen Akademie der Technischen Wissenschaften (SATW) die Schweizer Version des GCA Cybersecurity Toolkits für KMU lanciert. Das Toolkit bietet Unternehmen kostenlose und effektive Werkzeuge inklusive Anleitung für einen sicheren Umgang im Internet. Wie sehen diese Werkzeuge aus?
Das NCSC war im Projektteam dabei und hat es bei der Erarbeitung des Toolkits unterstützt. So wurde beispielsweise der KMU-Schnelltest überarbeitet und für die KMU noch attraktiver gestaltet (https://ictswitzerland.ch/themen/cyber-security/check/). Der vorliegende Schnelltest ermöglicht den Unternehmen eine Standortbestimmung und zeigt ihnen auf, ob sie die wichtigsten technischen, organisatorischen und mitarbeiterbezogenen Massnahmen für einen minimalen Cybersecurity-Schutz umsetzen. Eine umfassende und komplette Analyse steht jedoch nicht im Vordergrund. Gerade auch Zahnarztpraxen mit wahrscheinlich eher wenig ausgeprägten Kenntnissen bezüglich Informatiksicherheit, können sich so unkompliziert und schnell ins Bild setzen.

Welches sind die Neuerungen der Cybersecurity-Schnelltests für KMU gegenüber der Vorversion?
Wie bereits erwähnt, wurde der Schnelltest vereinfacht und attraktiver gemacht. Die Fragen wurden umformuliert und gekürzt. Somit müssen die Ärztinnen oder Ärzte nur ein paar wenige Minuten investieren, um eine ersten Eindruck ihrer Cybersicherheit in der Praxis zu bekommen. Das Resultat des Schnelltest sollte zum Anlass genommen werden, um dies mit dem IT-Verantwortlichen oder der externen Firma, welche die IT der Praxis betreut, zu diskutieren. Dies ist der erste Schritt für ein gemeinsames Verständnis und fördert den sicheren Umgang mit Informationen und Daten.

Die SSO hat zusammen mit der FMH einen Leitfaden für den IT-Grundschutz von Praxen entwickelt. Was halten Sie davon?
Ich begrüsse diese Initiative und fordere die SSO auf, weiter am Ball zu bleiben. Der Leitfaden muss regelmässig auf seine Aktualität überprüft und gegebenenfalls angepasst werden. Die Angreifer schlafen nicht, also müssen auch wir alle uns immer wieder der aktuellen Situation anpassen und rasch reagieren können.