Oberarzt Psychiatrie gesucht, Trojaner gefunden

Es begann mit einer besorgten Meldung unseres Kollegen Jürg Unger im Zentralvorstand. Psychiatrische Kliniken haben Schwierigkeiten, Kaderstellen mit qualifizierten Ärztinnen und Ärzten zu besetzen. Blindbewerbungen über das E-Mail sind deshalb interessant. Das Problem war nur, dass diesen Sommer eine solche Blindbewerbung das Betriebssystem der Klinik beinahe lähmte. Im Anhang fand sich nicht das versprochene Curriculum Vitae, sondern das trojanische Pferd. Zum Personalmangel gesellte sich also noch ein ernstes Informatikproblem. Schadprogramme, so genannte Malware, gibt es schon länger. Trojanische Pferde in E-Mail-Dateianhängen gehören zu den Klassikern. Neuer ist nur, dass mit der rasch fortschreitenden Digitalisierung in Praxen und Kliniken die Betriebssysteme von Gesundheitsinstitutionen häufiger und gezielt gehackt werden. Spezifisch für diese Institutionen ist, dass sie fast ausschliesslich sensible Daten verwalten. Datenschutz und Datensicherheit kosten hier nicht bloss Geld und Zeit; sie sind auch Bedingung für das Vertrauen von Patientinnen und Patienten und für eine hohe Behandlungsqualität.

Wir nehmen die berechtigte Sorge von Jürg Unger zum Anlass, mit einer lockeren Serie von Beiträgen zu Chancen und Risiken im dynamischen Bereich «Digitalisierung und e-Health» zu berichten. Wenn möglich möchten wir Experten und Expertinnen zu Wort kommen lassen. Den Anfang macht Pascal Lamia von MELANI.

Yvonne Gilli
Dr. med., Mitglied des FMH-Zentralvorstandes, Departementsverantwortliche Digitalisierung / eHealth

Ransomware auch im Gesundheitswesen

eHealth Aktuell

Pascal Lamia

Leiter der Melde- und Analysestelle Informationssicherung (MELANI)

Bei *Ransomware* (auch «Sperrtrojaner» oder «Erpressungstrojaner» genannt) handelt es sich um eine bestimmte Familie von Schadsoftware (Malware). Diese verbreitet sich üblicherweise über schädliche E-Mail-Anhänge (z.B. Bewerbungsdossier, Mahnungen fehlender Zahlungseingang, UPS-Paketzustellung etc.) oder gehackte Webseiten.

Einmal infiziert, verschlüsselt *Ransomware* Dateien auf dem Computer des Opfers sowie auf allfällig verbundenen Netzlaufwerken und Speichermedien (z.B. externe Harddisks, USB-Sticks). Die verschlüsselten Dateien werden dadurch für das Opfer unbrauchbar. Wurden die Dateien auf dem Computer erst einmal durch die Ransomware verschlüsselt, zeigt diese dem Opfer einen «Sperrbildschirm» an. Dieser fordert das Opfer auf, eine bestimmte Geldsumme in Form einer Internetwährung (beispielsweise Bitcoins) an die Angreifer zu bezahlen, damit diese die verschlüsselten Dateien wieder frei geben und somit wieder verwendet werden können (Erpressung).

Zahlung meistens in Bitcoins

Durch die Verwendung einer Internetwährung wie beispielsweise Bitcoins wird die Nachverfolgung der Urheberschaft erschwert. Ein Nachkommen der von den Angreifern gestellten Forderung und der damit verbundenen Zahlung an die Angreifer gibt jedoch keine Garantie, dass Opfer wieder Zugang zu den verschlüsselten Dateien erhalten. Zudem finanziert eine Zahlung das Geschäftsmodell der Angreifer und erlaubt diesen damit, die Angriffe mit *Ransomware* fortzuführen und weitere Opfer zu infizieren und zu schädigen.

Ransomware ist kein neues Phänomen: Bereits im Jahre 2011 ist die erste Ransomware in der Schweiz aufgetaucht, welche den Computer des Opfers sperrte und ein Lösegeld von ihm verlangte.

Drastischer Anstieg von Geschädigten

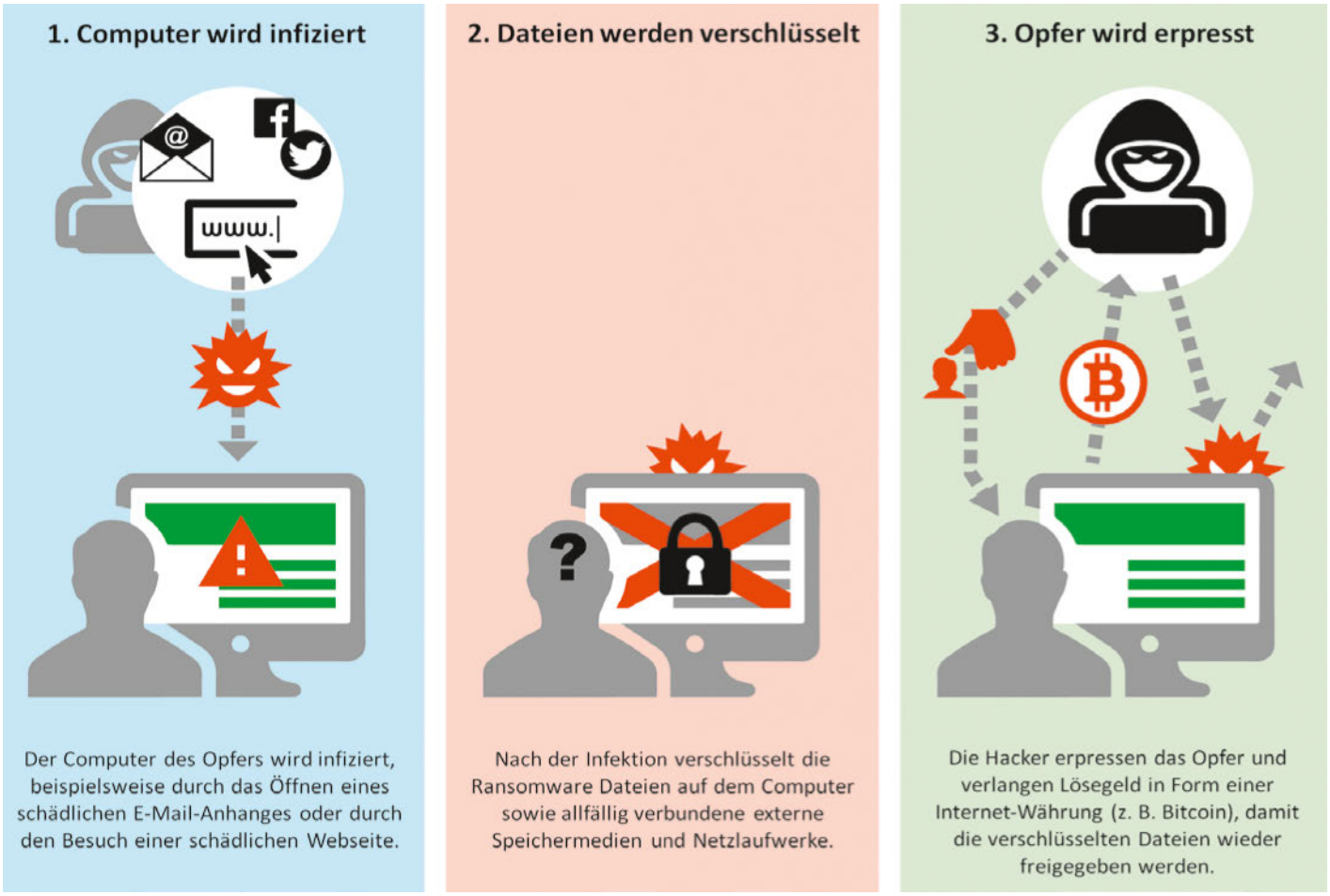
In den letzten Monaten hat sich die Zahl der Opfer von Ransomware in der Schweiz jedoch drastisch erhöht. Unlängst sind nicht nur Privatanwender Ziel von Angriffen mit Ransomware, sondern vermehrt auch kleine und mittlere Unternehmen (KMU), sowie vor allem auch im Gesundheitswesen (Spitäler).

Während Privatanwender bei einem Vorfall mit Ransomware nicht mehr auf ihre persönlichen Daten zugreifen können, sind die Auswirkungen für Unternehmen, insbesondere in Spitälern oder Arztpraxen, bei einem Ransomware-Vorfall in der Regel deutlich gravierender. Oftmals werden unternehmenskritische Daten wie beispielsweise Verträge, Kunden- und Buchhaltungsdaten, Patientendaten verschlüsselt und so unbrauchbar. Dies kann ein Spital oder eine Arztpraxis

Pascal Lamia

Pascal Lamia leitet die Melde- und Analysestelle Informationssicherung MELANI des Bundes. MELANI ist ein Kooperationsmodell zwischen dem Informatiksteuerungsorgan (ISB) und dem Nachrichtendienst (NDB), welche dem Finanzdepartement respektive dem Departement für Verteidigung, Bevölkerungsschutz und Sport zugeordnet sind.

Bildnachweise
Grafik und Foto zVg vom Autor



schnell einmal in eine Notlage bringen, was diese dann leider oftmals dazu animiert, ein Lösegeld zu bezahlen, um den Zugriff auf deren Daten wieder zu erlangen.

Dies muss nicht sein. Mit folgenden drei Massnahmen können Bürgerinnen und Bürger, aber auch KMU sich vor Ransomware schützen:

Sicherheitstipps

Erstellen Sie regelmässig eine Sicherungskopie (Backup) Ihrer Daten. Die Sicherungskopie sollte offline, das heisst auf einem externen Medium wie beispielsweise einer externen Festplatte, gespeichert werden. Stellen Sie daher sicher, dass Sie das Medium, auf welches Sie die Sicherungskopie erstellen, nach dem Backup-Vorgang vom Computer trennen. Ansonsten werden bei einem Befall durch Ransomware möglicherweise auch die Daten auf dem Backup-Medium verschlüsselt und unbrauchbar.

Seien Sie vorsichtig im Umgang mit E-Mails. Öffnen Sie keine E-Mail-Anhänge, welche Sie unerwartet bekommen oder dessen Absender Sie nicht kennen, und klicken Sie auf keine Links.

Halten Sie installierte Software und Plug-ins immer aktuell. Stellen Sie sicher, dass sämtliche installierte Software, Apps sowie auch Web-Browser-Plug-ins (Beispielsweise Flash Player, Java) stets auf dem aktuellen Stand sind. Verwenden Sie, wenn immer möglich, die automatische Update-Funktion der jeweiligen Software.

Detailliertere Informationen zu Ransomware und wie Sie sich vor solcher schützen können, finden Sie auf folgender Webseite der Melde- und Analysestelle Informationssicherung MELANI: https://www.melani.admin.ch/ransomware

Verhaltensregeln im Umgang mit Computern und dem Internet sowie zusätzliche Massnahmen zur Erhöhung der IT-Sicherheit in KMU sind unter folgenden Links abrufbar:

- **Verhaltensregeln:** https://www.melani.admin.ch/verhaltensregeln
- **Merkblatt IT-Sicherheit für KMU:** https://www.melani.admin.ch/it-sicherheit-fuer-kmus
- **10-Punkte-Programm zur Erhöhung der IT-Sicherheit:** https://www.kmu.admin.ch/kmu/de/home/praktisches-wissen/kmu-betreiben/infrastruktur-und-it/fachgerechte-it-infrastruktur/it-sicherheit.html

Korrespondenz:
FMH Verbindung der Schweizer Ärztinnen und Ärzte
Abteilung Digitalisierung / eHealth
Elfenstrasse 18
Postfach 300
CH-3000 Bern 15
Tel. 031 359 11 11
ehealth[at]fmh.ch