

Angriff auf die Praxissoftware

Rebekka Höhl Die Maschen von Cyberkriminellen werden immer ausgeklügelter. Im Trend liegen Erpressungs-Trojaner, die die kompletten Daten auf den infizierten Rechnern verschlüsseln. Von den Attacken sind längst auch Ärzte betroffen. Doch Praxen können vorbeugen.

Neu-Isenburg. Ob "Locky" oder "TeslaCrypt": Derzeit machen Verschlüsselungs-Trojaner die große Runde. Was das für den Praxisbetrieb bedeuten kann, musste erst kürzlich ein Internist erfahren: "Stellen Sie sich vor: Sie arbeiten in Ihrer großen Praxis mit mehreren Kollegen und Kolleginnen und vielen Mitarbeiterinnen, es ist viel los... und plötzlich sterben im Minutentakt die einzelnen Rechner der Mehrplatzanlage mit 18 Arbeitsplätzen ab", berichtet er. Man bange und hoffe auf den herbeieilenden Netzwerkadministrator, und der sagt schlicht: "Herr Doktor, Sie haben ein größeres Problem. Soeben wurden Ihre Praxisdaten verschlüsselt."

Damit liegt der Praxisbetrieb zumindest teilweise lahm. Schuld ist eine sogenannte Ransomware, ein Schadprogramm, das den Zugang zum Computer oder mobilen Geräten verhindert oder wie im Fall des Internisten die gespeicherten Daten verschlüsselt. Übertragen werden diese Schadprogramme über E-Mail-Anhänge und mitgeschickte Links (in beiden Fällen meist als eilige Rechnung getarnt) oder aber über angebliche Software-Updates.

Auch Cyber-Viren mutieren

Wie ausgeklügelt und vielfältig die Tricks der Cyberkriminellen mittlerweile sind, zeigt der Bericht des Bundesamtes für Sicherheit in der Informationstechnologie (BSI) zur IT-Sicherheit in Deutschland für 2015. Auf über 439 Millionen schätzt das BSI die Gesamtzahl der Schadprogrammvarianten. Dabei würden sich immer mehr dieser Varianten automatisch während der Weiterverbreitung auf den Rechnern generieren - fast so, wie lebende Viren mutieren. Aufgrund seines hohen Marktanteils sei zwar hauptsächlich Microsofts Betriebssystem Windows betroffen. Da Eintrittstor aber oft der Adobe Flash Player und eben E-Mail-Anhänge sind, sind auch Apple-Rechner nicht komplett außen vor.

Einbußen im fünfstelligen Bereich

Die Erpresser präsentieren sich "dreist und frech", wie der internistische Kollege erzählt, mit einem auf der Festplatte abgelegten Schreiben. Gegen Zahlung eines Geldbetrages würde die Freischaltung der verschlüsselten Daten veranlasst. Die Lösegeldzahlung für die Praxisdaten solle in Bitcoins - einer digitalen Währung - erfolgen.

Doch weil es keine Garantie dafür gibt, dass die Daten anschließend auch tatsächlich entschlüsselt werden, hatte sich zumindest der Kollege dazu entschlossen, nicht zu zahlen. Der Plan: Das Team wollte die Praxisdaten selbst rekonstruieren. "Was selbstverständlich mit einem erheblichen finanziellen und zeitlichen Aufwand verbunden ist. Hinzu kommt der Umsatzausfall für circa drei geschlossene Praxistage - ohne EDV können moderne Praxen nicht mehr betrieben werden. Hier sind schnell fünfstellige Einbußen erreicht", berichtet er.

Vor allem aber müssen die Daten noch an anderer Stelle vorliegen. Das Stichwort lautet Datensicherung. Dazu rät auch das BSI gerade wegen der in den vergangenen Wochen gehäuften Fälle von Ransomware-Attacken auf kleinere Betriebe und Privatpersonen. Laut BSI hat es erst im letzten Jahr auch das System eines Klinikkonsortiums hierzulande getroffen. Hier hatte die Schadsoftware Cryptowall zugeschlagen. Weil in großen Kliniken die Datensicherung meist ein Standardprozess ist, konnte der Datenausfall hier allerdings auf zwölf Stunden begrenzt werden.

Die Spielregeln für die Datensicherung sind dabei recht einfach:

- Sie sollte in der Tat regelmäßig (je nach Praxisgröße täglich bis wöchentlich) auf einem externen Speichermedium vorgenommen werden. Hierzu eignen sich etwa gut RAID-Systeme (Redundant Array of Independent Disks). Dahinter verbirgt sich ein Verbund unabhängiger Festplatten in einem Gehäuse. Die Daten werden beim Speichern gleichzeitig auf mehreren Festplatten abgelegt. Das senkt das Risiko, dass sie in irgendeiner Form nicht auslesbar sind. In kleinen Praxen kann aber auch eine normale USB-Festplatte für die Datensicherung genutzt werden.
- Die Datensicherung sollte immer getrennt vom Rechnersystem der Praxis aufbewahrt und vor allem nicht dauerhaft an dieses angeschlossen werden. Denn: "Viele Verschlüsselungstrojaner können auch Daten auf externen Laufwerken und Netzwerklaufwerken unbrauchbar machen", mahnt das BSI.
- Außerdem sollte das Praxisteam anhand einiger ausgewählter Dateien prüfen, ob sich die gesicherten Dateien tatsächlich wiederherstellen lassen und die Datensicherung funktioniert.

Auf Mehrfach-Schutz setzen

Zusätzlich benötigen Praxen Schutzmechanismen, die die Eindringlinge von vornherein abwehren. Dazu zählen in jedem Fall eine aktivierte, aktuelle Firewall (die meisten Internet-Router besitzen bereits eine integrierte Firewall), ein aktuell gehaltener Antivirens Scanner sowie ein Betriebssystem und ein Internetbrowser, die ebenfalls durch regelmäßige Updates auf dem aktuellen Sicherheitsstand gehalten werden.

Wichtig ist laut BSI aber ebenso eine gesunde Portion Misstrauen gegenüber unbekannten E-Mail-Absendern. Vor allem, wenn die Mails eine Rechnung "von einem Ihnen unbekannten Dienstleister" enthalten. Beim Surfen im Internet hilft es zudem, wenn der Virens Scanner sichere und unsichere Websites kennzeichnet, etwa mit grünem und rotem Symbol. Praxen müssen außerdem beachten, dass auch für die Patientendaten auf den Rechnern die Schweigepflicht gilt. Es gilt daher, die Systeme - falls der Nachweis doch einmal strafrechtlich nötig ist - nach bestem Gewissen - also aktuellem Stand der Technik, zu schützen.


707 Millionen Datensätze erbeuteten Cyberkriminelle im vergangenen Jahr weltweit - mit 1673 Hackerangriffen. 23 Prozent der Angriffe und 19 Prozent aller erbeuteten Daten entfielen auf den Gesundheitsbereich. Das zeigt eine aktuelle Studie von Gemalto, einem Anbieter von digitalen Sicherheitsdiensten. Das Unternehmen hat dazu die weltweiten Datenangriffe aus öffentlich zugänglichen Quellen analysiert.

Mehr zur Studie unter: www.aerztezeitung.de/905822

Quelle:	Ärzte Zeitung Nr. 54 vom 18.03.2016, Seite 10
ISSN:	0175-5811
Ressort:	Wirtschaft
Dokumentnummer:	000907372

Dauerhafte Adresse des Dokuments: https://www.wiso-net.de/document/AEZT__000907372

Alle Rechte vorbehalten: (c) Ärzte Zeitung Verlagsgesellschaft mbH

 © GBI-Genios Deutsche Wirtschaftsdatenbank GmbH