Cyberkriminalität

Apotheker gelten für Hacker als solvente Kundschaft

APOTHEKE ADHOC, 01.04.2019 09:08 Uhr

Sensible Daten: Apotheken sind laut Hans-Wilhelm Dünn vom Cyber-Sicherheitsrat als Schnittstelle zum Patienten im Visier von gezielten Hackerangriffen. Foto: Andreas Domma

***Berlin* - Cyberkriminelle haben es längst nicht nur auf Banken, Behörden oder Unternehmen abgesehen. Gesundheitsdaten stehen im Fokus. „Im Darknet werden hohen Preise für sensible Patientendaten gezahlt, die beispielsweise die dortigen Preise von Kreditkartendaten massiv übersteigen“, sagt Hans-Wilhelm Dünn, Präsident des Cyber-Sicherheitsrats Deutschland. Auch Apotheken bleiben als Schnittstelle zum Patienten von gezielten Angriffen nicht verschont.**

Welche Arzneimittel werden verschrieben? Welche Krankheiten haben die Patienten? Welche OTC-Produkte werden im Kundenkonto eingetragen? All diese Fragen seien interessant für Cyberkriminelle, erklärt Dünn. Die Daten würden als Nutzerprofile gebündelt verkauft. „Dadurch können Märkte beeinflusst werden.“ Nicht nur große Versandapotheken stünden im Visier. „Auch kleine Landapotheken werden gezielt angegriffen.“ Inhaber gelten für Hacker als „potenziell solvente Kundschaft“.

Den Kriminellen ginge es nicht um große Beträge, stattdessen machten sie mit vielen kleinen Forderungen ihr Geld. Ransomware – also Erpressungssoftware – werde in das Computersystem der Apotheke eingeschleust. Dadurch könne der Zugriff auf die Daten sowie die komplette Nutzung verhindert werden. Im Anschluss erhalte der Apotheker den Hinweis, Beträge zwischen häufig 200 und 1000 Euro für die Freischaltung zu zahlen. „Diese Angriffe sollten unbedingt bei der Polizei gemeldet werden“, appelliert Dünn, auch wenn die Strafverfolgung mit hohem Aufwand und langen Verfahren ohne Garantie auf Erfolg verbunden ist.

Oft werde Apothekern wie anderen Kleinunternehmern erst nach einem ersten Angriff bewusst, die eigenen Sicherheitssysteme der Betriebssoftware zu hinterfragen. „Dabei kommt häufig heraus, dass nur ein minimaler Schutz vorhanden ist.“ Wichtig sei, dass nicht allein der Chef ein Bewusstsein für vermeintliche Angriffe entwickle. „Auch die Mitarbeiter müssen regelmäßig informiert werden. Sie sind häufig eine Schwachstelle.“

Vor allem über infizierte Links und Anhänge in E-Mails führen Hacker dem Verein Cyber-Sicherheitsrat Deutschland zufolge erfolgreiche Angriffe durch. „Durch einen Systemausfall kann nach wenigen Tagen ein Liquiditätsengpass erreicht werden, der großen Schaden für den Betrieb bedeuten kann.“ In die Öffentlichkeit dringen die Attacken nur selten. „Die daraus resultierenden immensen Reputationsverluste können das Weiterbestehen des Betriebs gefährden“, so Dünn.

Apotheken profitierten derweil von der Zusammenarbeit mit Softwarehäusern. Die EDV-Anbieter berücksichtigen die Thematik Cybersicherheit stärker. „Bei den Dienstleistern herrscht naturgemäß eine hohe Sensibilität für Datenschutz und Internetsicherheit.“ Dünn empfiehlt, gemeinsam mit den Anbietern das Thema regelmäßig kritisch zu hinterfragen. „Es lohnt sich, auch einmal andere Unternehmen auf das eigene System schauen zu lassen, um herauszufinden, ob der eigene Dienstleister noch up to date ist.“

2017 wurden vom Bundesamt für Sicherheit in der Informationstechnik (BSI) insgesamt 800 Millionen Schadprogramme für Computersysteme identifiziert. Höhere Budgets seien für eine effektive Strafverfolgung, angemessene Cybersicherheitsvorkehrungen und einen starken Cybersicherheitsmarkt nötig. Zudem müssten Lehrpläne entsprechend angepasst und Lehrstühle geschaffen werden, um dem enormen IT-Sicherheitsfachkräftemangel entgegenzuwirken.