Die vernachlässigte Gefahr aus dem Internet

Die Gesundheitsbranche als Ziel von Hackern

Viele Arztpraxen, Pflegeheime, Pflegedienste und Kliniken fühlen sich vor Cyberkriminalität gewappnet / Doch die Angreifer sind sehr professionell und die Bedrohung ist gigantisch / Von Mark Peters

Berlin, 05. April

Als der Hackerangriff das Pflegeheim und den ambulanten Pflegedienst in Thüringen erschüttert, sind auf den Pflegestationen alle Mitarbeiter alarmiert.

Krankeninformationen und hochsensible Patientendaten in den falschen Händen können zu finanziellen Schäden und eine Gefährdung für Leib und Leben von Patienten führen, das wissen alle.

Der EDV-Fachmann, der eigentlich für IT-Sicherheit zuständig ist konnte nicht helfen. Die internen Entscheider waren im Urlaub und es war Ostern. Die Katastrophe kam von einer Sekunde auf die andere.

Dies wurde bekannt, weil das Pflegeheim sehr transparent über den Angriff berichtet und darüber, wie seine Mitarbeiter mit der Attacke jetzt nach der gezielten Cyberabwehr-Schulung von Praxismanagement Bublitz-Peters umgehen.

Die Angreifer hatten eine Ransomware im System platziert, das ist ein Verschlüsselungstrojaner, mit dem Lösegeld erpresst wird (z. B. „LockerGoga“). Die Idee der Kriminellen: Für Chaos sorgen und Druck aufbauen, damit das Lösegeld gezahlt wird.

v. r. n. l. Geschäftsführerin Silke Bublitz-Peters von Praxismanagement Bublitz-Peters, Kriminalhauptkommissar Herr Olaf Borries LKA Berlin, Referent Mark Peters von Praxismanagement Bublitz-Peters

Auf dem SpiFa-Fachärztetag 2019 in Berlin www.bublitzpeters.de/2019/05/02/spifa-fachaerztetag-2019-2/ hat die Ärzteschaft die Empfehlung aufgegriffen und führt gemeinsam mit Praxismanagement Bublitz-Peters sensibilisierende Fortbildungen und Schulungen in Deutschland durch.

Auch das PKV Institut aus München nutzt für Ihre Zahnärzte und Ärzte die Kompetenz von Praxismanagement Bublitz-Peters. Z. B. im MFA exklusiv Magazin vom Mai 2019 „ Datenschutz praktisch“- so schützen Sie sich sicher gegen Cyberkriminalität“ bzw. mit regelmäßigen Datenschutzveröffentlichungen.

Den meisten Praxen und Pflegeeinrichtungen ist klar, dass sie irgendwann angegriffen werden, die Frage ist nur wann und wie schwerwiegend die Folgen eines Angriffs sind. Wie man sich vor Cyber-Kriminalität schützt erklären Praxismanagement Bublitz-Peters und das LKA Berlin, siehe Abbildung.

„Vor allem Ransomware-Angriffe nehmen zu, weil sie so häufig erfolgreich sind. Und die Hacker geben sich mehr Mühe. Sie studieren ihre Opfer für eine lange Zeit und ich würde Unternehmen raten, niemals zu bezahlen und man weiß nicht, wen man mit dem Lösegeld finanziert“ so Olaf Borries.

Die Betreiber von Botnetzen, mit denen Cyberangriffe automatisiert werden können, arbeiteten heutzutage sehr professionell. Wenn es nicht funktioniert, spricht sich das schnell in der Branche herum.

Laut Herrn Kriminalhauptkommissar Olaf Borries, LKA,Berlin, zeigt die Cybersicherheitsumfrage des Bundesamts für Sicherheit in der Informationstechnik (BSI), dass jedes dritte deutsche Unternehmen von Attacken betroffen ist. In der Hälfte der Fälle waren die Angreifer laut BSI erfolgreich. Sie konnten sich zum Beispiel Zugang zu IT-Systemen verschaffen oder Internetauftritte manipulieren. In vielen Fällen sei es zu Betriebsstörungen oder –ausfällen gekommen. Hinzu kamen häufig noch die Kosten für die Aufklärung und Wiederherstellung der Systeme und zudem der Schäden für die eigene Reputation. Trotzdem sehen nur 8 % der gut 1000 Unternehmen und Institutionen, die das BSI befragt hat, ihre Betriebsabläufe in Gefahr. In viel zu wenigen Unternehmen gibt es Übungen, einen Notfallplan oder einen Cyber-Beauftragten.

Fachleute wie Herr Kriminalhauptkommissar Olaf Borries vom LKA oder Mark Peters von Praxismanagement Bublitz-Peters sehen das als großes Problem. Jede Arztpraxis, Klinik oder Pflegeheim oder jedes Unternehmen hat verschiedenen EDV und IT Systeme im Einsatz. Die Betreuung erfolgt meist durch eine Vielzahl von Unternehmen oder auch in eigener Arbeit z.B. durch die Ärzte oder Leiter der Einrichtungen.

Die Kliniken, Arztpraxen oder Pflegeheime haben oftmals Fachabteilungen mit betreffenden beauftragten Personen (z.B. Hygiene-, Arbeitsschutz, Datenschutz, Abrechnungsbeauftragte), aber ein Cyber-Beauftragter fehlt zu 99 %.

„Die Arbeitsteilung, die in der Cybercrime-Szene auf eine große Fachqualität im Angriff ausgerichtet ist wird ebenfalls von den Unternehmen im Gesundheitswesen unterschätzt“, so Mark Peters, Datenschutzexperte bei Praxismanagement Bublitz-Peters. Seit gut 10 Jahren ist er für den Bereich Datenschutz- und Cybersicherheit verantwortlich. Es werden nun Sensibilisierungslösungen für den Bereich der Phishing-Mails angeboten.

Sein Mittel ist, mit Ärzten oder verantwortlichen Mitarbeitern mögliche Angriffe in einem Planspiel durchzusprechen. Mittendrin erkennen die Kunden, dass sie in Schwierigkeiten sind, entweder weil es zu wenig professionelle Unternehmen oder Mitarbeiter gebe oder keine richten Abläufe. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt vor einer deutlichen Zunahme des sogenannten „Mail-Spoofings“. Dabei senden Cyberkriminelle Verbrauchern E-Mails mit vermeintlich vertrauenswürdigen Absender-Identitäten – zum Beispiel der eines Kollegen, Geschäftspartners oder Bekannten.

Praxismanagement Bublitz-Peters GmbH & Co. KG betreut seit mehr als 15 Jahren über 3.000 Leistungserbringer im Gesundheitswesen und bietet für SIE gute, günstige und pragmatische Lösungen, sowie die Möglichkeit ESF-Förderungen in Anspruch zu nehmen.

https://www.bublitzpeters.de/

Praxismanagement Bublitz-Peters empfiehlt, dass jedes Unternehmen Cyberkompetenz im Rahmen eines Cyber-Beauftragten aufbaut oder zumindest von außen einkaufen sollte. Die Sensibilisierung der Mitarbeiter ist das A und O in der Schadensvermeidung.

Heidelberger-Datenschutz-Rating:

https://www.hcm-magazin.de/rating-gibt-es-jetzt-auch-virtuell/150/10980/387358