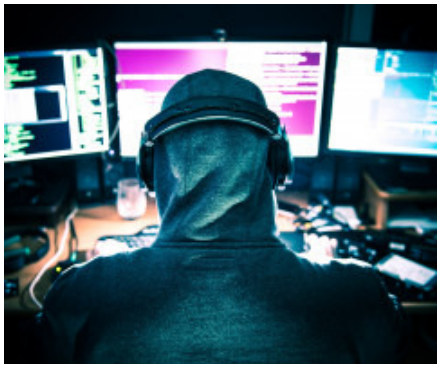
Digitalisierung

Wie die digitale Notaufnahme nicht zum digitalen Notfal wird

Wie schütze sich Krankenhäuser besser gegen Cyberangriffe? Wie der Expertenvortrag am dritten Ta der Jahrestagung Deutsche Gesellschaft Interdisziplinäre Notfall- und Akutmedizin (DGINA) zeigte, können Kliniken sehr effektiv verhindern, dass ihre digitalen Notaufnahmen nach einem Hackerangrif selbst zu digitalen Notfällen werden. Technik ist dabei längst nicht alles. Auch das machten die beide IT-Sicherheitsberater von „DigiTrace“ aus Köln in ihrem Beitrag deutlich.



Bei der Jahrestagung der DIGNA sprachen Experten darüber, wie man sich von Cyberangriffen von Hackern schützen kann.

(c) Pterzayda, Adobe Stock

Ein komplexer Hacker-Angriff lässt sich nicht mit einer Firewall oder eine Virenscanner entdecken, geschweige denn abwehren. Das war die schlechte Nachricht, die Martin Wundram und Alexander Sigel für alle hatten, die sich von ihrem Online-Vortrag einfache Lösungen versproche hatten. Doch hatten sie einige gute Vorschläge, wie Krankenhäuser die realen Risiken der digitalen Welt deutlich reduzieren können.

„Besser in Köpfe investieren“, lautet dabei ihre wichtigste Schutzmaßnahme. Konkret denken sie an die Ausbildung von Mitarbeite zu digitalen Ersthelfern. Dadurch könnten medizinische Notdienste den gröbsten Fehler vermeiden, den viele Unternehmen machen: durch Nichtstun wertvolle Zeit zu verlieren. Genau diese Haltung hat Martin Wundram, der seit 10 Jahren als Sachverständiger für IT-Sicherheit und Forensik für Gerichte, Staatsanwaltschaften, Polizeibehörden, Unternehmen und Privatpersonen tätig ist, in der Praxis sehr häufig beobachtet.

Digitale Ersthelfer, die darin geschult seien, frühestmöglich Vorfälle zu erkennen und geeignete Maßnahmen durchzuführen, könnten größeres Unheil verhindern. „Damit lastet nicht alles auf Schultern der IT-Abteilung c Leitung ihrer Klinik“, nennt Wundrams Co-Referent Alexander Sigel einen weiteren Vorteil. Zum Zeitaufwand Ausbildung konnte er auf Nachfrage lediglich einen groben Rahmen nennen. Er gehe davon aus, dass „mindestens ein Arbeitstag“ eingeplant werden müsse. Plus einmal im Jahr ein Tag für eine IT-Notfallübung. Damit sei das Geld besser investiert als „in die IT-Schrankware“, wie sie üblicherweise gekauft werde, ist er überzeugt.

Außerdem sei es ratsam, regelmäßig die Effektivität der Schutzlösungen durch Penetrationstests zu prüfen, denen beauftragte IT-Experten simulierte Angriffsversuche durchführen. Dringend empfahl der Experte seine Zuhörern zudem eine strikte Trennung von System und Netzwerk, um nicht vertrauenswürdige Bereiche (Browsen im Internet, E-Mail-Anhänge) und Patientendaten und andere vertrauliche Informationen zu trenne

13.11.2020 15:53, Autor: bfe, © änd Ärztenachrichtendienst Verlags-AG
Quelle: https://www.aend.de/article/208921