

Technologie

In dieser Ausgabe



Christoph Schäfer
Secorvo Security Consulting
Verschlüsselung funktioniert
Trendscout
Seite 397



Neltje Piro
Hochschule Ulm
Pioniere der Teleklinik
Smartphone-Einsatz für Telemonitoring
Seite 398



Prof. Dr. Michael Reiher
Hochschule Nürtingen-Geislingen
Wissensvorsprung am Keyboard
Klinik-IT-Umfrage zur Weiterbildung
Seite 402



Peter Carqueville
Redaktion f&w
Das nächste Ziel der Klinik-Hacker
Sicherheitslücken in der Medizintechnik
Seite 406

Außerdem im Ressort Technologie:

Markt
Neues aus der Industrie
Seite 410

Trendscout

Verschlüsselung funktioniert



Von Christoph Schäfer

Während die Verschlüsselung von Daten im Unternehmens- und Krankenhausalltag nach wie vor kaum etabliert ist, funktionierte sie bei den aktuellen Erpresser-E-Mails bestens. Die Nachrichten enthielten Verschlüsselungstechniken wie TeslaCrypt 3 oder Locky und kamen in Gestalt sogenannter Trojaner. Die kleinen Programme schleusen sich beispielsweise über Word-Dokumente als E-Mail-Anhang ins Unternehmensnetz ein. Öffnet der unbedarfte Nutzer den E-Mail-Anhang, beginnt die Software fleißig damit, alle Dateien zu verschlüsseln, auf die der Nutzer Zugriffsrechte hat. Ist sie fertig, folgt eine Lösegeldforderung. Die US-amerikanische Bundespolizei FBI rät dazu, solche Lösegelder zu zahlen.

In der Vergangenheit ließen sich beispielsweise von TeslaCrypt 2 verschlüsselte Dateien noch wiederherstellen, da der dazu benötigte digitale Schlüssel rekonstruierbar in der Datei versteckt wurde. Die neue Generation von Ransomware, die sich seit Anfang 2016 verbreitet, ist leider besser geworden. Auch ältere Erpressungstrojaner wie Cryptowall setzen inzwischen wirksame kryptografische Verfahren ein. Ohne den nötigen Schlüssel an die Dateien zu gelangen, ist nicht möglich oder braucht zumindest sehr viel mehr Zeit, als man auf seine Daten verzichten kann. Auch die E-Mails, mit denen die Trojaner einherkommen, sind heutzutage professionell aufgemacht und frei von Rechtschreibfehlern früherer Tage, an denen man sie noch leicht erkennen konnte. Heute sind E-Mails meist persönlich adressiert und passen auch im Inhalt zum Arbeitsumfeld des Empfängers.

Braucht es also neue Schutzmaßnahmen? Muss die Krankenhaus-IT komplett auf den Kopf gestellt werden? Ganz pauschal lautet die Antwort erst mal „Nein“. Dennoch rächen sich nun die Sünden der Vergangenheit. Der Schadsoftware, die aus simplen E-Mails heraus relativ ungehindert ihre Arbeit verrichten konnte, wurde es vermutlich durch relativ offene Netzlaufwerke innerhalb der Kliniken zusätzlich leicht gemacht. Es gilt zu bedenken: Die geöffnete Schadsoftware arbeitet im Krankenhausnetz mit denselben Zugriffsrechten wie ihre Opfer.

Warum muss eigentlich der Chefarzt auf alles zugreifen können? Müssen alle Mitarbeiter mit Admin-Rechten arbeiten, die ihnen die ungehinderte Installation beliebiger Software erlaubt? Und wie ist es mit der Datensicherung? Hat das eigene Haus regelmäßige und wiederherstellbare Backups, verlieren auch die Verschlüsselungstrojaner große Teile ihres Schreckens. Das alles ist kein Hexenwerk sondern eigentlich das ABC der Informationssicherheit.

Vor allem aber kommt es auf die Mitarbeiter an. Der gesunde Menschenverstand, kombiniert mit Sensibilisierungsmaßnahmen, ist der beste Schutz gegen solche Angriffe. Nicht nur logisch, sondern schlicht wahr ist: Werden verseuchte E-Mail-Anhänge gar nicht erst geöffnet, werden auch die Infektionen unterbunden. Das ist wirkungsvoller als jeder Virenschutz, der neue Varianten der Trojaner ohnehin meist mehrere Stunden lang nicht blockiert. Schließlich müssen zunächst Tausende Systeme infiziert sein, damit die Schutzsoftware den neuen Schädling kennenlernt. Dumm gelaufen, wenn das ausgerechnet Ihre Systeme sind. Natürlich wissen auch die Entwickler, wie die Verteidiger arbeiten und passen ihre Schadsoftware regelmäßig an. Qualifizierte Mitarbeiter sind letztlich der beste Schutz.

Der Autor ist Datenschutzexperte der Secorvo Security Consulting GmbH.

Autoren dieser Kolumne

Christoph Schäfer
Secorvo Security Consulting
GmbH

Martin Schleicher
Paul Gerhardt Diakonie Berlin

Dr. Hajo Reißmann
Universitätsklinikum
Schleswig-Holstein

Norbert Ruch
Fachverband für
Krankenhauseinkäufer (femak)

Prof. Dr. Thomas Lenarz
Deutsche Gesellschaft für
Biomedizinische Technik

Bernd Christoph Meisheit
Sana IT Services

Prof. Dr. Ursula Hübner
Hochschule Osnabrück

Dr. Sebastian Wibbeling
Fraunhofer-Institut für
Materialfluss und Logistik IML