COMPUTER IM WÜRGEGRIFF: BEDROHUNGEN UND GEGEN-STRATEGIEN

Ein Klick auf den Anhang der neuen E-Mail und das Verhängnis nimmt seinen Lauf: Der Rechner ist gesperrt, alle Daten sind nur noch Kauderwelsch und der Erpresser schreibt „Bitcoins her oder das war's." Inzwischen bekanntgewordene Fälle zeigen, dass Angriffe durch Ransomware auch vor dem Gesundheitswesen nicht Halt machen. Mit Vorbereitung, Bedacht und kühlem Kopf kann man dieser Bedrohung jedoch entgegentreten.

Als „Ransomware" wird eine Familie von Schadprogrammen aus E-Mails oder dem Internet bezeichnet, die alle Nutzdaten eines Anwenders verschlüsseln und nur gegen Zahlung von Lösegeld wieder freigeben. Diese Angriffe sind zwar schon seit Jahren bekannt, sind aber gerade im letzten Jahr deutlich häufiger geworden und greifen inzwischen wie ein Krebsgeschwür die Daten aller am Opfer angeschlossenen Speichersysteme an.

Die Nutzdaten werden dabei nicht gelöscht, sondern „nur" verschlüsselt. Sie stehen damit auch nach Beseitigung des angreifenden Schadprogramms nicht mehr zur Verfügung. Dabei erfolgt die Verschlüsselung in der Regel so effizient, dass die Entschlüsselung nur noch mithilfe des kriminellen Erpressers möglich ist, die dieser sich teuer bezahlen lässt. Oft wird der Druck durch den Anhang einer Zeitbombe noch intensiviert und mit der endgültigen Datenlöschung gedroht. Das „Geschäft" soll dann schnellstens über anonyme Zahlungsmittel wie Bitcoin oder Guthaben- und Bezahlkarten direkt mit dem Täter abgewickelt werden.

Gegenüber bisheriger klassischer Schadsoftware, wie zum Beispiel Banking-Trojanern oder Identitätsdaten-Diebstahl, ist für das Opfer der wesentliche Unterschied, dass der Schaden unmittelbar eintritt und auf Dauer verheerende Konsequenzen haben kann. Alle Unternehmensdaten auf den angegriffenen Rechnern sind ab sofort gesperrt und stehen nicht mehr zur Verfügung. Die geforderte Zahlung an den Erpresser ist in jedem Fall hoch. Aber auch nach der „Lösegeldübergabe" gibt es keine Garantie für eine Freigabe des Rechners, denn nicht alle Angreifer sind so „ehrlich" und liefern danach auch tatsächlich den Schlüssel für ihr Schloss.

Bedrohungslage

Aktuelle Forschungsberichte weisen darauf hin, dass diese Bedrohungen die Fachwelt zunehmend beschäftigen. Meist auf Amerika fokussiert, beziehen sich aber viele der internationalen Studien aufgrund seiner Bedeutung als Datenstandort ausdrücklich auf Deutschland. Statistiker haben untersucht, welcher Versorgungssektor am meisten betroffen ist. Die Durchdringung mit Ransomware ist demnach in der Gesundheitsversorgung am höchsten, gefolgt von Finanzdienstleistungen, Produktion und Regierungen, mit jeweils absteigender Intensität. Interessant ist, dass die Angriffshäufigkeit auf einzelne Unternehmen mit ein bis fünf Attacken pro Jahr nahezu überall sporadisch ist. Nur weniger als ein Prozent der Unternehmen wird häufiger und gezielter angegriffen. Es handelt sich somit um ein Massenphänomen nach dem „Schrotschuss-Prinzip" mit nur sehr seltenen strategischen Angriffen auf bestimmte Ziele.

Seit Dezember letzten Jahres beobachtet das Bundesamt für Sicherheit in der Informationstechnik (BSI) große Angriffswellen von Ransom-

ware in Deutschland. Als häufigste sogenannte Angriffsvektoren gelten hierzulande Spam, also unerwünschte E-Mails mit Schadpaketen im Anhang, außerdem sogenannte Drive-by-Infektionen – also unbeabsichtigtes Herunterladen von Schadsoftware beim Surfen auf präparierten Webseiten, Schwachstellen von Servern, das heißt ungepatchte oder veraltete Software, und schließlich ungeschützte Fernwartungszugänge, sodass Internet-Protokoll-Scans offene Fernzugänge suchen und finden.

Angriffe von Ransomware nehmen aus immer ähnlichen Motiven zu, denn trotz der nur vergleichsweise seltenen „Erfolge“ ist laut BSI das Geschäftsmodell für Angreifer immer rentabel und zwar aus zwei Gründen: Es entsteht ein hoher Leidensdruck bei den Opfern – für Geschädigte sind die Wiederherstellungsaufwände oft größer als die Erpressersumme. Außerdem sind die Zahlungen in Bitcoins anonym und sofort in Bargeld umsetzbar. Der Angreifer verschwindet somit im Nebel.

Vorbeugende Maßnahmen

Der Erfolg der Ransomware beruht fast ausschließlich auf groben Versäumnissen bei der Prävention, denn viele der Angriffe sind nicht mit großem programmtechnischen Aufwand gestaltet. Schlecht gepflegte Systeme, fehlende, veraltete oder nicht hinreichend überprüfte Software-Backups, schwache Administratoren-Passworte oder die fehlende Aufteilung der Netzwerke rächen sich sofort durch den dann eintretenden Schaden. Das Verhalten der Mitarbeiter der betroffenen Betriebe spielt dabei eine zentrale Rolle. So könnte allein schon eine bessere Sensibilisierung die Systeme wesentlich widerstandsfähiger machen. Aufmerksamkeit, Vorsicht und Vorsorge erweisen sich hier als wichtigste Waffen.

Das BSI widmet den Maßnahmen zur Vorbeuge ein eigenes Kapitel in seiner neuen Broschüre „Ransomware, Bedrohungslage, Prävention & Reaktion“. Dort findet sich ein ganzes Arsenal wirksamer Ansätze gegen die Feinde unserer informationstechnischen Infrastruktur. Dabei darf sich für die Heilberufe durchaus ein Déjà-vu-Erlebnis einstellen, denn das Ganze liest sich wie der Abschnitt „Prävention“ aus der klinischen Infektiologie: Hygiene, Abwehrstärkung, Ansteckungsvermeidung und Vorsorge.

Dabei steht eine Schutzmaßnahme immer an erster Stelle: Sicherung, Sicherung und nochmals Sicherung. Dies gehört zwar schon seit Langem zu den selbstverständlichen informationstechnischen Grundschutzkonzepten. Die Sicherung gewinnt aber angesichts dieser neuen Bedrohung nochmals an Bedeutung. Hinzu kommt, dass jetzt die gesicherten Daten in einem sogenannten Offline-Backup abgelegt werden müssen, da viele Ransomware-Varianten auch Online-Backups, wie Daten auf NAS-Systemen oder Schattenkopien verschlüsseln. Es genügt also nicht mehr wie bislang empfohlen, die räumlich getrennte Aufbewahrung, solange Rechner und Sicherungen über ein Fernnetz weiter online miteinander verbunden bleiben. Natürlich gehören zum Gesamtkonzept die Planung des Wiederanlaufs und die regelmäßige Überprüfung der Sicherungsdaten.

Reaktionsmaßnahmen

Wenn es dann doch einmal zu einem Sicherheitsvorfall mit Ransomware gekommen ist, gilt es, wie auch in der Intensivmedizin, ruhig zu bleiben und mit Bedacht zu handeln. An vorderster Front steht die Empfehlung des BSI: auf eigene Vorbereitungen zurückgreifen und nie, nie bezahlen. Diese letzte Empfehlung hat zwei Aspekte: Der externe Grund ist, dass jede erfolgreiche Erpressung den Angreifer weiter motiviert und für noch größere Verbreitung sorgt. Der interne Grund ist, dass der Betroffene bei geeigneter Vorbereitung sehr wahrscheinlich Geld einspart.

Konkret sind erkennbar infizierte, möglicherweise mitinfizierte, genauso wie gesunde Systeme umgehend voneinander zu trennen. Es gilt, die Schäden zu begrenzen, den Infektionsherd zu finden, das System dort neu aufzusetzen, die Sicherungsdaten wiederherzustellen und die Veränderungen seit der letzten Sicherung in Ruhe nachzutragen.

Weder dieser Beitrag noch das Merkblatt des BSI können alle Fragen und Handlungsoptionen rund um das heikle Thema Ransomware abschließend beantworten. Dafür gibt es Experten und externe Unterstützung. Eines sollte aber spätestens aus den ärztlichen Medien deutlich geworden sein: Die Datentechnik der Gesundheitsversorger lebt nicht mehr in einem unangreifbaren Elfenbeinturm. Konnektoren, Firewalls und virtuelle private Netzwerke können Datentechnik zwar schon wesentlich sicherer machen, aber die größte Schwachstelle sitzt meist vor dem Bildschirm.

Dr. med. Christoph Goetz, Leiter Gesundheitstelematik (KVB)

Literatur zum Thema

- Die im Beitrag genannte Broschüre „Ransomware, Bedrohungslage, Prävention & Reaktion“ des Bundesamts für Sicherheit in der Informationstechnik (BSI) finden Sie unter www.bsi.bund.de.
- Weitere Informationen: Osterman Research, Understanding the Depth of the Ransomware Problem in the United States, Juli 2016. https://go.malwarebytes.com/OstermanRansomwareSurvey.html