Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Veröffentlichungen zur Cyber-Sicherheit

EMPFEHLUNG: METHODIK

Schutz vor Ransomware

Präventive Maßnahmen zur Absicherung vor Krypto-Trojanern

1 Ausgangslage

Zu Beginn des Jahres 2016 berichtete die Presse vermehrt über Ransomware-Infektionen in Deutschland – Krankenhäuser und andere Institutionen, aber auch Privatpersonen waren von diesen Vorfällen betroffen. Derartige Schadprogramme verschlüsseln Daten auf den Rechnern der Opfer sowie möglicherweise weiteren angeschlossenen Laufwerken und verlangen zur Wiederherstellung die Zahlung eines Lösegelds.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beobachtet täglich kurzzeitige, massive Spam-Wellen, deren E-Mail-Anhänge sog. Downloader beinhalten. Diese z. B. als Word-Dokumente oder JavaScript getarnten Dateien laden nach dem Öffnen unbemerkt Schadprogramme, wie die oben beschriebene Ransomware, nach.

Ist es zu einer Infektion gekommen und liegt kein Backup vor, stehen die Betroffenen vor dem Problem, wieder Zugriff auf die verschlüsselten Daten zu erlangen. Die Erfolgsaussichten variieren mit der jeweiligen Ransomware-Variante. Gelegentlich gelingt es Sicherheitsforschern, verschlüsselte Daten eigenständig wiederherzustellen. Entsprechende Anleitungen und Tools werden anschließend im Internet veröffentlicht. Es kann sich daher lohnen nach Hilfestellungen im Web zu suchen.

Die von den Kriminellen verlangte Zahlung sollte nach Meinung des BSI grundsätzlich nicht getätigt werden. Einerseits ist nicht sicher, dass die Täter nach Erhalt des Lösegelds tatsächlich den benötigten Schlüssel liefern, andererseits ist nicht auszuschließen, dass nach der ersten Überweisung Nachforderungen vonseiten der Kriminellen zu erwarten sind. Stattdessen sollte in jedem Fall die Polizei kontaktiert und Anzeige erstattet werden. Eine Liste der Kontaktstellen [1] finden Sie auf der Webseite der Allianz für Cyber-Sicherheit.

Damit nicht erst nach einer Infektion mit kostenintensiven Maßnahmen zur Datenrettung begonnen werden muss, sollten im Vorfeld Sicherheitsvorkehrungen getroffen werden, die eine kurzfristige Wiederherstellung der Daten erlauben.

2 Präventive Gegenmaßnahmen

Nach jetzigem BSI-Kenntnisstand ist die einzig wirksame Maßnahme zum Schutz vor vollständigem Datenverlust das Anlegen von Backups. Diese müssen regelmäßig angefertigt, stichprobenartig auf ihre Funktion geprüft und unabhängig vom IT-Netz gela-

gert werden. Informationen zur Datensicherung und zur Erstellung eines entsprechenden Konzepts finden Sie im BSI IT-Grundschutz Baustein CON.3 [2].

Die Notwendigkeit zur separaten Lagerung resultiert insbesondere aus der Erfahrung, dass einige Krypto-Trojaner nicht nur die lokalen Daten ihres Opfers, sondern auch diejenigen Daten verschlüsseln, auf die von dort aus zugegriffen werden kann. Mithilfe durchdachter Netz-Segmentierungen innerhalb des Unternehmens und restriktiv eingesetzter Firewalls können derartige Szenarien abgewendet werden, grundsätzlich sorgt jedoch die Speicherung auf einem externen Datenträger für die höchste Sicherheit. Anregungen zur Erstellung eines Netzkonzeptes finden Sie im BSI IT-Grundschutz Baustein NET.1.1.A3 oder auch NET.1.1.A16 [3].

Eine weiterer Faktor zur Vermeidung eines Ransomware-Ausbruchs im Unternehmensnetz ist die restriktive Vergabe von Benutzerrechten. Durch die Reduzierung von Zugriffsmöglichkeiten auf Verzeichnisebene kann die abteilungsübergreifende Verschlüsselung von Daten in einer Organisation vermieden werden. Weitere Informationen liefert der BSI IT-Grundschutz Baustein APP.2.1.A3 [4].

Um das Risiko einer Infektion mit Schadsoftware im Vorhinein zu minimieren, empfiehlt sich außerdem die regelmäßige Schulung von Mitarbeitern. Insbesondere Abteilungen, in denen häufig E-Mail-Anhänge von unbekannten Absendern geöffnet werden – z. B. in Personalabteilungen eingehende Bewerbungen – gelten als besonders exponiert. Aber auch beim Öffnen von E-Mails vermeintlich bekannter Verfasser sollte stets auf Unregelmäßigkeiten geachtet werden, schließlich könnte sich ein Angreifer z. B. Zugriff auf das Postfach des Absenders verschafft haben. Sind die Mitarbeiter in der Lage, bösartige E-Mails vor dem Öffnen zu erkennen, bedeutet dies einen signifikanten Sicherheitsgewinn für die Unternehmens-IT. Weitere Informationen finden – u. a. zur Erkennung von E-Mail-Angriffen – finden Sie in den Angeboten der Allianz für Cyber-Sicherheit.

Dieses Ziel kann auch durch die Filterung/Markierung von E-Mails mit Anhängen, z. B. ausführbaren Dateien, unterstützt werden.

Generell ist zu beachten, dass E-Mail nicht der einzige Verbreitungsweg für Ransomware ist. Auch Drive-by-Downloads und unzureichend geschützte Netzwerkkomponenten gehören zu den häufig genutzten Methoden. Aufgrund dessen gelten auch hier die gängigen Schutzmaßnahmen für IT-Systeme. Dazu zählen u. a.:

- Sichere Konfiguration der eingesetzten Betriebssysteme: Hier bietet die Allianz für Cyber-Sicherheit auf ihrer Webseite Sicherheitsempfehlungen zu Windows, Apple OS X und Linux an.
- Nutzung von Anti-Viren-Software
- Sichere Konfiguration der eingesetzten Software: z. B. durch Deaktivierung von Makros in Office-Produkten und Nutzung der Sandbox von pdf-Readern.
- aktuelle Patchstände der eingesetzten Soft- und Hardware: Prüfen Sie die Webseiten der Hersteller regelmäßig auf Sicherheitsaktualisierungen und spielen Sie diese zeitnah ein.
- Sichere Konfiguration von Netzwerkkomponenten, wie auch deren Fernwartungszugänge [5].

3 Weitere Informationen

Im Jahr 2016 hat das Bundesamt für Sicherheit in der Informationstechnik das Themenpapier „Ransomware – Bedrohungslage, Prävention & Reaktion“ [6] veröffentlicht. Dort finden sich weiterführende Informationen, insbesondere zur Bedrohung durch Ransomware und zu reaktiven Maßnahmen im Angriffsfall.

4 Links

[1] Allianz für Cyber-Sicherheit: „Zentrale Ansprechstellen Cybercrime“ bei den Polizeien: https://www.allianz-fuer-cybersicherheit.de/ACS/ZACs

[2] IT-Grundschutz: Entwicklung eines Datensicherungskonzepts: https://www.bsi.bund.de/dok/10095836 sowie https://www.bsi.bund.de/dok/10095932

[3] IT-Grundschutz: Entwicklung eines Netzkonzeptes: https://www.bsi.bund.de/dok/10095830

[4] IT-Grundschutz: Einrichtung von Zugriffsberechtigungen auf Verzeichnisdienste: https://www.bsi.bund.de/dok/10095796

[5] Allianz für Cyber-Sicherheit: Grundregeln zur Absicherung von Fernwartungszugängen: https://www.allianz-fuer-cybersicherheit.de/dok/6649756

[6] Bundesamt für Sicherheit in der Informationstechnik: Themenpapier Ransomware – Bedrohungslage, Prävention & Reaktion: https://www.bsi.bund.de/dok/7714940

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an **info@cyber-allianz.de** gesendet werden.