Ransomware
Eine aktuelle und stetig steigende Bedrohung

Norbert Pohlmann

Laut dem Bericht „Die Lage der IT-Sicherheit in Deutschland 2021“, herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik (BSI), ist eine spürbare Ausweitung Cyberkrimineller Erpressungsmethoden, etwa mittels Ransomware, aktuell festzustellen.

Ransomware ist eine böswillige Schadfunktion in Malware, die Daten auf dem jeweils kompromittierten IT-System (Notebooks, PCs, Smartphone, Server…) verschlüsselt. Ziel eines Angreifers ist es, die Nutzung der Daten oder des ganzen IT-Systems durch die Verschlüsselung zu unterbinden. Dadurch kann der Angreifer vom Besitzer des IT-Systems oder der IT-Systeme für den Schlüssel, mit dem die Daten entschlüsselt werden können oder/und das IT-System wieder freigegeben wird, Lösegeld verlangen.

Das Lösegeld wird in der Regel über digitale Währungen wie Bitcoin oder andere Kryptowährungen bezahlt. Eine Möglichkeit zur Festlegung der Lösegeldforderung ist, dass die Angreifer dafür öffentlich verfügbare Informationen wie etwa der Unternehmensgröße, Umsatz und Gewinn nutzen. Bei Privatleuten wird in der Regel ein fester Betrag, oftmals 500 Euro, festgelegt.

Synonyme für Ransomware sind Erpressungstrojaner, Erpressungssoftware, Kryptotrojaner oder Verschlüsselungstrojaner.

Der Angriffsvektor Ransomware ist momentan sehr aktuell und wird zunehmend mehr eingesetzt, da er ermöglicht, einen sehr hohen Schaden auf unterschiedlichen Ebenen zu verursachen.

Beispiele von Ransomware-Angriffen auf Unternehmen:

Benzinpipeline in den USA
Der Betreiber der größten Benzinpipeline in den USA, Colonial Pipeline, zahlte Hackern ein Lösegeld von 4,4 Millionen Dollar. Der Ransomware-Angriff hatte zur Folge, dass die Kraftstoffversorgung landesweit vorübergehend eingeschränkt war.

Uniklinikum Düsseldorf
Den Angreifern gelang es, 30 Server des Uniklinikums zu verschlüsseln. Dadurch konnte das Klinikum die zentrale Notversorgung nicht mehr sicherstellen, sodass circa 1000 Patienten in umliegenden Krankenhäusern untergebracht werden mussten. Eine Notfallpatientin, die in eine weiter entfernte Klinik gebracht wurde, verstarb kurze Zeit später.

Funke Mediengruppe
Angreifer verschlüsselten mehrere IT-Systeme des Verlags im gesamten Bundesgebiet. Die Zeitungen „Westdeutsche

Allgemeine Zeitung“, „Hamburger Abendblatt“ und „Berliner Morgenpost“ konnten aufgrund der Ransomware-Attacke nur als Notausgabe erscheinen.

Kammergericht Berlin
Mehr als 500 Computer und über hundert Server mussten wegen einer Ransomware-Attacke vom Netz genommen werden. Daraus resultierte, dass das Kammergericht über mehrere Monate nur per Telefon, Fax oder Brief erreichbar war.

Wichtig ist die Planung von Gegenmaßnahmen:
Dazu gehören unter anderem bereits getestete Reaktionskonzepte (Notfallplanungen), in denen sowohl die richtige Vorgehensweise für den Angriffsfall definiert ist als auch bestimmten Personen die entsprechenden Rechte zuzuweisen, um die notwendigen Maßnahmen zu ergreifen. Besonders relevant ist dabei, alle definierten Reaktionen gemeinsam im Detail zu trainieren, damit im Ernstfall schnell und erfolgreich agiert werden kann.
Daneben lässt sich durch ein vollständiges, und auf Wiederherstellung geprüftes, Backup der IT-Systeme in vielen Fällen ein Schaden verhindern oder zumindest minimieren.
Das BSI unterscheidet in seinem Bericht zwei unterschiedliche Erpressungsmethoden bei Ransomware, die einzeln oder zusammen (Double Extation) Anwendung finden werden.

Lösegelderpressung:
Cyber-Erpresser verschlüsseln IT-Systeme und fordern Lösegeld für die Schlüssel, damit durch eine Entschlüsselung, dass IT-System wieder nutzbar ist.

Schweigegelderpressung:
Dies ist eine erweiterte Angriffsstrategie dahingehend, dass vor der Verschlüsselung von Daten diese zunächst unrechtmäßig entwendet wurden. Unternehmen, die über funktionierende Backups verfügten und sich von daher theoretisch nicht auf Lösegeldverhandlungen einlassen müssten, wird dann mit der Veröffentlichung der entwendeten Daten gedroht, um so das Schweigegeld zu erpressen.

Dies bedeutet, im Fall eines Ransomware-Angriffs muss nunmehr grundsätzlich auch davon ausgegangen werden, dass die Daten dauerhaft kompromittiert sind und zwar auch dann, wenn ein Lösegeld oder/und Schweigegeld gezahlt worden ist.

Aus diesem Grund ist der beste Schutz vor Ransomware, alle IT-Systeme mit einer modernen und sicheren Anti-Malware Lösung auszustatten und alle Mitarbeiter/Nutzer dahingehend zu schulen, dass sie aufgrund ihres Sicherheitsbewusstseins nicht auf gängige Angriffsvektoren reinfallen – also weder auf Anhänge von unbekannten/unaufgefordert zugesandten E-Mails noch auf Links von manipulierten Webseiten klicken. Aber auch das systematische Überwachen des Datentransfers hilft, ungewöhnliche Aktivitäten zu erkennen und so das Stehlen von Daten zu verhindern. Dies ist ein essenzieller Schritt, um das Risiko zu minimieren Opfer einer Schweigegelderpressung zu werden.

Fazit: Die Brisanz des Angriffsvektors zeigt, dass sich Unternehmen und Privatleute generell mit den Möglichkeiten sowie der Vermeidung von Ransomware-Angriffen auseinandersetzen müssen, damit sie alles tun, um einen Schadensfall zu vermeiden.

Prof. Dr. Norbert Pohlmann ist Professor für Cyber-Sicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco. Außerdem ist Prof. Pohlmann Mitglied des wissenschaftlichen Beirates der Gesellschaft für Datenschutz und Datensicherung – GDD und Mitglied im Lenkungskreis der Initiative „IT-Sicherheit in der Wirtschaft“ des BMWi sowie Mitglied der Advisory Group der European Union Agency for Cypersecurity der ENISA. 2011 wurde es als „Professor des Jahres“ in der Kategorie Ingenieurswissenschaften/Informatik“ ausgezeichnet.

Im Sommersemester 2013 war er als Gastprofessor an der Stanford University im Fachbereich Computer Science, Silicon Valley, USA. Die vielfältigen Fachartikel sowie mehrere Lehr- und Sachbücher auf dem Gebiet der Cyber-Sicherheit dokumentieren seine Passion für das Gebiet und machen ihn zu einem nachgefragten Experten für Interviews und Diskussionen.