Die Gefahr lauert überall: Hacker haben Spitäler im Visier

Cyberattacken erfordern schnelle und effektive Reaktion

Hackerangriffe auf Krankenhäuser sind kein Einzelfall mehr. Aber wie sollen sie bei einem Sicherheitsvorfall reagieren? Orientierungshilfe geben Best Practices, die Sicherheitsexperte NTT Security zusammengestellt hat.

Erst im Februar dieses Jahres gerieten mehrere Krankenhäuser wegen Hackerattacken in die Schlagzeilen, so das Lukaskrankenhaus in Neuss, bei dem es zu massiven Störungen im Netzwerk kam und sogar Operationen verschoben werden mussten.

IT-Verantwortlichen im Gesundheitsbereich wird zunehmend klar, dass ihre bisherige Sicherheitsstrategie Grenzen aufweist, wenn vor allem bei der schnellen Reaktion auf Hacker-Angriffe noch einiges im Argen liegt. Das Thema «Incident Response» rückt deshalb verstärkt ins Blickfeld.

Es braucht eine Sicherheitsstrategie

Klar ist, dass die Abwehr eines Angriffs nicht erst beim Sicherheitsvorfall selbst beginnen darf. Eine Sicherheitsstrategie muss deshalb auch ein Incident-Response-Verfahren mit detaillierten Ablauf- und Notfallplänen für die Behandlung von unterschiedlichen Vorfällen beinhalten. Hier sollten beispielsweise Verantwortlichkeiten festgelegt, Aufgaben definiert, Schadensfälle klassifiziert oder Kommunikationsmassnahmen geregelt werden.

Doch welche Massnahmen sind dann im Ernstfall, sprich beim Incident, konkret zu ergreifen? Sicherheitsexperte NTT Security empfiehlt die Einhaltung von folgenden fünf Best Practices:

1. Identifizierung

Zunächst muss geklärt werden, um welchen Vorfall es sich handelt. Zur Analyse können zum Beispiel Log-Files – auch aus SIEM (Security Information and Event Management)-Systemen – herangezogen werden. Zudem ist zu ermitteln, welche Zielsysteme betroffen sind, welchen aktuellen Status der Angriff hat und inwieweit bereits das gesamte Unternehmensnetzwerk kompromittiert ist.


Bild: NTT Security

Der Autor Patrick Schraut ist Director Consulting & GRC bei NTT Security in Ismaning.

2. Beenden des Angriffs

Der zweite Schritt umfasst das Stoppen beziehungsweise Eindämmen der Attacke. Abhängig vom Angriffsszenario sind unterschiedliche Massnahmen denkbar, vom Abschalten einzelner Systeme über das Abtrennen bestimmter Netzwerkbereiche bis hin zu einem vollständigen Kappen aller Internetverbindungen.

3. Wiederherstellung

Der dritte Schritt sieht die Beseitigung aller Schäden vor. Dabei muss die IT alle Systeme, die

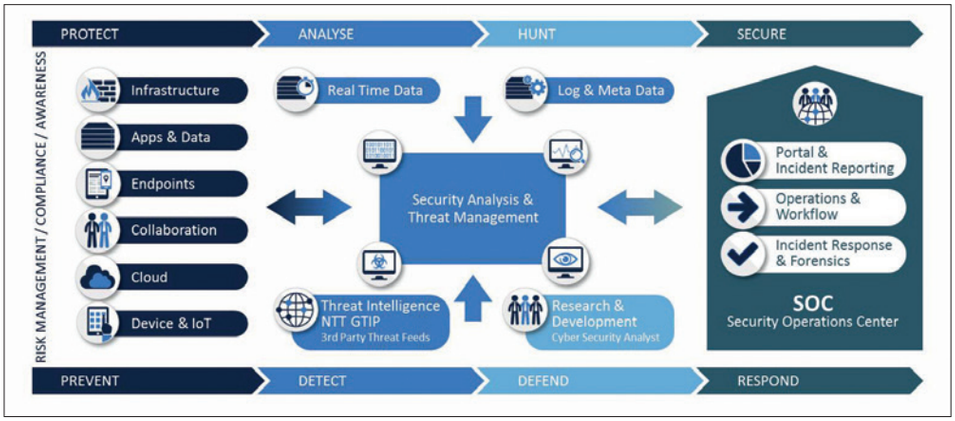
potenziell betroffen sind, detailliert untersuchen. Das betrifft Betriebssysteme, Applikationen und Konfigurationsdateien ebenso wie alle Anwenderdateien. Zur Überprüfung eignen sich nur Sicherheitstools, die auf dem neuesten Stand sind, etwa aktuelle Antivirenlösungen. Bei Datenverlust muss die IT entsprechende Recovery-Massnahmen ergreifen.

4. Aufnahme des Normalbetriebs

Der nächste Schritt umfasst die Wiederaufnahme des Normalbetriebs, beispielsweise mit der sukzessiven Zuschaltung aller abgeschalteten Subsysteme. Vor der Wiederinbetriebnahme müssen dann auf jeden Fall umfassende Testläufe erfolgen, in denen der reibungslose Systembetrieb überprüft wird – zum Beispiel mittels Anwendungsfunktionstests.

5. Dokumentation und Massnahmeneinleitung

Der letzte Schritt betrifft die Aspekte Dokumentation und Massnahmeneinleitung. Eine Dokumentation muss eine klare Bestandsaufnahme des vergangenen Incidents enthalten sowie eine detaillierte Bewertung der ergriffenen Aktivitäten. Auf dieser Basis kann ein Unternehmen dann entsprechende Massnahmen ergreifen, um einen Sicherheitsvorfall ähnlicher Art künftig zuverlässig auszuschliessen.



Die Cyber-Defense-Strategie von NTT Security basiert auf den vier Grundkomponenten Prävention, Erkennung, Abwehr und Reaktion. (Quelle: NTT Security)

Angesichts aktueller und steigender Sicherheitsbedrohungen kommt kein Krankenhaus an der Konzeption und Umsetzung einer Incident-Response-Strategie vorbei. Ist dies aus fachlichen oder personellen Gründen nicht möglich, sollte ein externer Dienstleister hinzugezogen werden, der im Bereich Cyber-Security entsprechende Referenzen vorweisen kann.

Text: Patrick Schraut, Director Consulting & GRC bei NTT Security in Ismaning