Lukaskrankenhaus Neuss sorgt mit Application Whitelisting Virenangriff vor

Schaden macht klug – mit Sicherheit

„Computer-Virus legt das Lukaskrankenhaus lahm." So titelte die Rheinische Post am 11. Februar 2016 in ihrer Onlineausgabe. Es war die Zeit des Verschlüsselungstrojaners Locky. Am Morgen des vorigen Tages hat die Einrichtung in Neuss bemerkt, dass Systeme sehr langsam und Funktionen zum Teil nicht mehr verfügbar waren sowie in gewissen Bereichen Daten verschlüsselt wurden. „Daraufhin haben wir unsere IT-Systeme vorsorglich heruntergefahren, um zu verhindern, dass das Virus Patientendaten befällt, ändert oder gar löscht", erläutert Bernd Zimmer, Abteilung IT im Lukaskrankenhaus. Mit spezialisierten Experten startete die IT dann die Suche nach dem Schädling und setzte parallel aus Backups die Systeme komplett neu auf.

Jan Lutz

Der Virenbefall und seine Folgen hatten erhebliche Auswirkungen auf den Betrieb im Lukaskrankenhaus. Die Klinik ist mit ihren zwölf Fachabteilungen ein wichtiger Leistungserbringer in und um Neuss. Das akademische Lehrkrankenhaus der Universität Düsseldorf hat 537 Betten und versorgt jährlich 28.500 Patienten stationär sowie 80.000 ambulant. „Wir wurden durch Locky sehr weit zurückgeworfen und konnten nicht auf gewohntem Niveau arbeiten. Hunderte Rechner waren vom Virus befallen", blickt Jan Lutz aus der Abteilung IT mit Schrecken zurück. „Durch das Neuaufsetzen der Systeme und Clients musste sehr viel Zeit investiert werden." Ausgelöst wurde die Attacke auf die Computersysteme des Krankenhauses durch einen geöffneten E-Mail-Anhang – und das nur wenige Tage nachdem das Bundesamt für Sicherheit in der Informationstechnik (BSI) vor dem Öffnen solcher Anhänge gewarnt hatte. Trotz aller Technik hatte der Mensch versagt. „Um die Risiken für die Zukunft zu verringern, hat das BSI uns geraten, eine Lösung zum Application Whitelisting einzuführen", erinnert sich Zimmer. Daraufhin brachte ERGO Computersysteme, mit dem das Lukaskrankenhaus bereits über Jahre zusammenarbeitet, SecuLution ins Spiel. „Wir haben uns die Software angeschaut und dann recht schnell entschieden, dass wir sie einsetzen wollen", sagt Lutz.

White- statt Blacklisting

So ist die Lösung nun sein April 2016 im Lukaskrankenhaus Neuss im Einsatz – und bietet den Anwendern und der IT-Abteilung ein hohes Maß an Sicherheit, wie Zimmer ausführt: „Heute ist es so, dass nur die Programme ausgeführt werden, die wir vorher als sicher eingestuft haben. Alle anderen, etwa unbekannte oder schadhafte Dateien, werden blockiert und wir bekommen einen entsprechenden Warnhinweis." Vorher hat sich das Haus auf eine Firewall und einen entsprechenden Virenscanner für das Mail-Programm verlassen. Was – wie die Erfahrung lehrt – heute offenbar nicht mehr ausreichend ist.

Schadprogramme verändern sich in sehr schneller Folge in Nuancen und können deshalb von den herkömmlichen Schutzprogrammen nicht entdeckt werden. Deshalb haben Virenscanner merklich an Wirksamkeit verloren. Mittels einer Blacklist kann immer nur das gefunden und blockiert werden, was bereits bekannt ist – sei es eine bestimmte Schadsoftware oder ein bestimmtes Verhalten. Sind die dem Virenscanner nicht bekannt, können Trojaner und ähnliches ungehindert in das Netzwerk gelangen und dort Schaden verursachen. Während ein Virenscanner also definiert, was verboten ist und alles Unbekannte erlaubt, verhält es sich beim Application Whitelisting genau umgekehrt: Es wird definiert, was zur Arbeit benötigt wird, alles andere kann nicht gestartet werden. Im Gegensatz zum Virenscanner muss SecuLution also nicht die neueste Version der Schadsoftware kennen, um ein Eindringen in das Netzwerk zu verhindern.

Aufwand lohnt sich

„Viele Vorteile für ein einziges Programm", meint auch Bernd Zimmer. Nach der schnellen Entscheidung für SecuLution folgte die ebenso schnelle Einführung. „Gut für uns, da wir aus nachvollziehbaren Gründen unter Zeitdruck standen", ergänzt Lutz. Mit der Implementierung hatte die IT des Hauses nicht zu tun, das haben komplett die Dienstleister übernommen – gut, wie Zimmer findet, „schließlich hatten wir zu dem Zeitpunkt ganz andere Sachen zu bedenken." Nach einer intensiven Schulung übernimmt nun aber die IT die gesamte Administration der Application-Whitelisting-Lösung.

Wie das funktioniert, erläutert Herr Zimmer: „Wir haben je einen separaten Rechner für die drei Betriebssysteme Windows 7, Windows 8 und Windows 10. Updates werden darauf dann über eine Web-Datei jede Nacht in SecuLution angelernt. Wenn das geschehen ist, rollen wir sie klinikweit aus und geben sie zur Nutzung frei – ansonsten würde SecuLution ja alle Dateien von Windows blockieren, die es nicht kennt." Interne Anwendungen wurden initial freigegeben, kommen neue hinzu, werden die individuell zugeschaltet. Häufig bekommt die IT-Abteilung entsprechende Anfragen von Anwendern, die eine bestimmte Applikation nutzen möchten, deren Ausführung aber geblockt wird. „Wir prüfen dann mit lediglich zwei Mausklicks, ob sie sicher ist und geben das Programm frei. Das können wir genauso einfach auch für mehrere Anwendungen gleichzeitig tun", erläutert Lutz.

Bernd Zimmer,

Was sich nach Arbeit für die IT anhört, bedeutet allerdings nur einen recht geringen Mehraufwand. „Jeder Virus kostet uns mehr Zeit", betont Zimmer. „In der Administration kommt etwas mehr auf uns zu, da wir jede einzelne neue Anwendung prüfen und in SecuLution freigeben müssen – und das mit gerade neun Mitarbeitern, die für die gesamte Infrastruktur, alle Informationssysteme im Haus sowie den klassischen Helpdesk verantwortlich sind. Allerdings gewinnen wir dadurch ein Höchstmaß an Sicherheit, was den Aufwand mehr als rechtfertigt." Neben der Überprüfung von ausführbarem Code lässt sich sogar die Verwendung von Geräten, die per USB an einen Computer angeschlossen werden, kontrollieren. Damit gehört die umständliche Verwaltung von USB-Ports und deren Freigabe der Vergangenheit an.

Wiederholung ausgeschlossen

Das ist auch eine Lehre, die das Lukaskrankenhaus Neuss aus Locky gezogen hat – Investitionen in die Sicherheit zahlen sich aus. Das zeigt auch das Beispiel SecuLution: Weil die Benutzer keine Software mehr ausführen können, die nicht beruflich benötigt wird, wurde das Risiko menschlichen Versagens bestmöglich minimiert. „Da jedoch keine IT-Lösung hundertprozentigen Schutz versprechen kann, versuchen wir weiterhin, die Mitarbeiter zu schulen und für den verantwortungsvollen Umgang mit der IT-Infrastruktur zu sensibilisieren", sagt Jan Lutz. Das geschieht in Neuss zum einen durch Plakate im gesamten Krankenhaus, die regelmäßig getauscht werden, zum anderen durch Videos und die persönliche Ansprache in Veranstaltungen. Budget sei dafür ausreichend vorhanden, wie überhaupt zur Wahrung der IT-Sicherheit. Und seit Locky deutlich mehr als vorher. In punkto Application Whitelisting steht der Sinn der Investition für Bernd Zimmer außer Frage: „Überall wo wir SecuLution installiert haben, kann uns so etwas wie Locky nie wieder passieren."