Öffentlicher Dienst

EVANGELISCHE PERTHES-STIFTUNG e.V.
menschennah.

GBS Success Story

Evangelische Perthes-Stiftung wehrt Verschlüsselungs-Trojaner in E-Mail-Anhängen mit iQ.Suite Convert ab

iQ.Suite

Das Unternehmen

Die Evangelische Perthes-Stiftung e.V. begleitet täglich mehr als 8.000 Menschen mit Unterstützungsbedarf und ist ein überörtlicher Träger diakonischer Einrichtungen für Menschen im Alter, Menschen mit Behinderungen, Menschen in besonderen sozialen Schwierigkeiten, Menschen mit Suchterkrankungen und Menschen in ihrer letzten Lebensphase. Die Stiftung ist mit 4.550 Mitarbeitern an 90 Standorten in Nordrhein-Westfalen vertreten.

Bereits seit 2008 ist die Perthes-Stiftung GBS Kunde und hat zur Absicherung ihrer E-Mail Kommunikation unter Microsoft Exchange verschiedene Module der E-Mail Security Lösung iQ.Suite im Einsatz: Watchdog (Viren-und Phishingschutz), Wall (Spamschutz), Trailer (gesetzeskonformes E-Mail-Footer Management) sowie Crypt Pro (serverbasierte E-Mail-Verschlüsselung).

Die Herausforderung

Durch die zunehmende Anzahl von Cyberattacken, insbesondere durch Ransomware (Erpressungs-Trojaner), steigen die Anforderungen an einen aktuellen und zuverlässigen Schutz der E-Mail-Kommunikation auch bei der Perthes Stiftung.

Ende 2016 löste der Verschlüsselungs-Trojaner GoldenEye ein großes Medienecho aus. Bei diesem Trojaner handelte es sich um eine besonders perfide Erpressungsmasche. GoldenEye tauchte hauptsächlich in Deutschland auf und wurde über den Anhang in E-Mails, meist getarnt als Bewerbungsschreiben, verbreitet. Diese E-Mails enthielten meist zwei Anhänge: Einen mit tatsächlichen, wenngleich gefälschten, Bewerbungsunterlagen, um den Schein zu wahren, und einen zweiten mit einer Excel-Datei. Sobald letztere geöffnet wurde und der Empfänger der Aufforderung nachkam, die „Bearbeitungsfunktion“ zu aktivieren, wurde der Angriff ausgelöst. Denn dies erlaubte es dem Programm, Makros auszuführen: GoldenEye wurde auf dem PC sofort aktiv und begann unbemerkt mit der Verschlüsselung der Festplatte seiner Opfer. Für die Entschlüsselung der Daten forderten die Erpresser Lösegeld. „Ich erinnere mich an den Virenangriff. Die Bewerbung machte auf den ersten Blick einen professionellen und überzeugenden Eindruck. Auffällig war, dass eine Excel-Datei beigefügt war, was bei Bewerbungen unüblich ist. Allerdings ist gerade auch im Kreis Soest zunächst jede eingehende Bewerbung im Pflegebereich höchst interessant, da die Akquise von Personal für die Pflege äußerst schwierig ist“, beschreibt Heike Pannewig, Einrichtungsleitung im Perthes-Zentrum Soest der Evangelischen Perthes-Stiftung e.V., die Situation. Gefragt war also eine zuverlässige Lösung zur effektiven Abwehr von Erpressungs-Trojanern.

GBS Success Story

Evangelische Perthes-Stiftung

iQ.Suite

Die Lösung

Mit iQ.Suite Convert bietet GBS eine Lösung zum zuverlässigen Schutz vor gefährlichem Schadcode. Die Installation, die lediglich einen Tag in Anspruch nahm, setzt auf die Fingerprint-Technologie. Im Zusammenspiel mit iQ.Suite Watchdog werden verdächtige Office Dokumente mit Makros erkannt, zunächst angehalten und mit iQ.Suite Convert in das PDF-Format umgewandelt.

Das nachfolgende Szenario zeigt, wie es der Perthes-Stiftung mithilfe von iQ.Suite Convert und der Antiviren-Lösung iQ.Suite Watchdog gelang, die gefährliche Ransomware GoldenEye erfolgreich abzuwehren:

Ausgangssituation

In der Verwaltung der diakonischen Stiftung geht eine Bewerbung mit einer Excel-Datei als Anhang per E-Mail ein. Eine Mitarbeiterin stuft die Bewerbung als echt und relevant ein und leitet die E-Mail an die Leitung der Einrichtung weiter.

So arbeiten beide Sicherheitslösungen zusammen

1 iQ.Suite Watchdog erkennt bei der eingehenden E-Mail potentiell verdächtige Makros im Excel-Dokument.

2 Die E-Mail wird angehalten, in Quarantäne gestellt und der Anhang mit iQ.Suite Convert in das PDF-Format umgewandelt.

3 Der Mitarbeiterin der Perthes-Stiftung wird der umgewandelte Anhang als PDF-Datei zugestellt. Dadurch stellt aktiver Schadcode keine Bedrohung mehr dar.

4 Im nächsten Schritt unterzieht iQ.Suite Watchdog den originalen E-Mail-Anhang einer erneuten Prüfung, mit den in der Zwischenzeit aktualisierten Antivieren-Signaturen.

5 Die Analyse erkennt nun GoldenEye. iQ.Suite Watchdog lehnt daraufhin die Zustellung der Datei ab, wodurch eine Infizierung der Festplatte des Computers verhindert wird.

Ergebnis

Der gefährliche Verschlüsselungs-Trojaner wurde rechtzeitig erkannt und blockiert. Wäre die Excel-Datei übrigens als ungefährlich eingestuft worden, dann wäre die Zustellung des Anhangs an den Empfänger im ursprünglichen Format erfolgt. „Ich bin sehr zufrieden: Die Installation der neuen Lösung iQ.Suite Convert ist problemlos verlaufen und wir sind noch einmal besser gegen Trojaner in Office-Dateien gewappnet“, sagt Marcus Staender, Stabsbereich Informationstechnologie, Evangelische Perthes-Stiftung.

„Die Installation der neuen Lösung iQ.Suite Convert ist problemlos verlaufen und wir sind noch einmal besser gegen Trojaner in Office-Dateien gewappnet“

***Marcus Staender** – Stabsbereich Informationstechnologie*

GBS Success Story

Evangelische Perthes-Stiftung

iQ.Suite

Der Mehrwert

Durch die Integration von iQ.Suite Convert sorgt die Perthes-Stiftung für Sicherheit auf höchstem Niveau und ist gegenüber neuartigen Bedrohungen durch Ransomware umfassend geschützt. Die zentrale PDF-Konvertierung verhindert zudem das Ändern von Dateien.

Da iQ.Suite Convert nicht am Arbeitsplatz installiert werden muss, sondern das Modul zentral und automatisiert vom Server aus gesteuert wird, werden die Mitarbeiter des diakonischen Werks in keinster Weise in ihrer täglichen Arbeit beeinträchtigt. Obendrein entfällt jeglicher Schulungsaufwand – ein wichtiger Aspekt beim produktiven Einsatz. Positiver Nebeneffekt: Durch Reduzieren der Größe von E-Mail-Anhängen wird die Netzwerk-Infrastruktur der Perthes-Stiftung entlastet.

Das Fazit

Mit der iQ.Suite hat die Perthes-Stiftung eine Lösung im Einsatz, welche die gesamte E-Mail-Kommunikation vor Cyberattacken schützt. Krypto-Trojaner werden zuverlässig erkannt und wirkungsvoll abgewehrt. Der gesamte Prozess läuft vollständig automatisiert und sorgt so für einen reibungslosen Betrieb. Um neuartige Ransomware abzuwehren, zieht die diakonische Stiftung aktuell den Einsatz der cloud-basierten Sandbox-Technologie von GBS in Betracht. Bei der innovativen Technologie handelt es sich um eine Erweiterung von iQ.Suite Watchdog. Neuartige Bedrohungen werden in einer abgesicherten Cloud-Umgebung dank dynamischer Verhaltensanalyse auf schadhaftes Verhalten untersucht und blockiert.