Das Magazin für Führungskräfte in Kirchen und kirchlichen Organisationen

www.kviid.de

KVI im DIALOG

1 | Februar 2020

Energie & Umwelt
Ein Klimaschutzkonzept für das Erzbistum Paderborn

SICHER

Informationssicherheit – sicher in das neue Jahrzehnt

Ein Beitrag von Christoph Dessel und Sascha Knauf

Christoph Dessel ist seit seinem Eintritt Anfang 2014 Leiter des Geschäftsfeldes IT-Audit von Curacon. In den zurückliegenden fast 20 Jahren hat Christoph Dessel nicht nur Komplexträger, Krankenhäuser und Unternehmen der Sozialwirtschaft sowie Einrichtungen der öffentlichen Hand im Rahmen von IT-Audits betreut, sondern auch bei einer Vielzahl von IT-Projekten begleitet und beraten.

Sascha Knauf betreut als verantwortlicher Wirtschaftsprüfer Mandanten unterschiedlicher Branchen, Rechtsformen und Größe. Sein Schwerpunkt liegt dabei in der Prüfung und Beratung von Komplexträgern, Wohlfahrtsverbänden sowie von Gebietskörperschaften und öffentlichen Unternehmen. Er ist Leiter des Ressort Öffentlicher Sektor und Kirche und wurde im Jahr 2019 in die Partnerschaft von Curacon aufgenommen und übernahm die Leitung der Niederlassungen in Ratingen und Saarbrücken.

Das Jahr 2019 war geprägt durch umfangreiche Angriffe auf Informationstechnologie. Schätzungen zufolge belaufen sich die Schäden in Deutschland auf rund 100 Mrd. Euro pro Jahr.[1] Wir werfen einen Blick auf die größten Bedrohungen des Jahres 2019 und leiten daraus Handlungsempfehlungen ab, wie sie sich erfolgreich vor zukünftigen Angriffen schützen können.

Lage der Informationssicherheit 2019

Jährlich veröffentlicht das Bundesamt für Sicherheit in der Informationstechnik (BSI) seinen Bericht zur Lage der Informationssicherheit in Deutschland.[2] Darin bewertet es die aktuelle Gefährdungslage, beschreibt Angriffsmethoden und geht auf Lösungen und Angebote zur Verbesserung der Informationssicherheit ein.

Wie in den Vorjahren war laut BSI auch 2019 die Infektion durch Schadsoftware die größte Bedrohung für die Informationssicherheit in Behörden, Unternehmen und bei Privatanwendern. Hier nennt das BSI explizit die Schadsoftware Emotet, auf deren Funktionsweise wir im folgenden Kapitel eingehen. Darüber hinaus waren Identitätsdiebstahl, Angriffe auf die Verfügbarkeit von Informationstechnik und das Versenden von Spam-Nachrichten als relevante Angriffsmethoden zu beobachten.

Interessant ist in diesem Zusammenhang eine aktuelle Umfrage zum Thema Informationssicherheit in Deutschland.[3] Die Bitkom e.V. befragte Führungskräfte von Unternehmen ab 10 Mitarbeitern. Die Befragung zeigte, dass die Anzahl der Angriffe auf Unternehmen in den letzten zwei Jahren signifikant zugenommen hat und auch die Anzahl der Angriffe, die zu einem tatsächlichen Schaden führten, sich nahezu verdoppelt hat.

Dabei hatten es die Angreifer auf Finanzdaten, Mitarbeiter- und Kundeninformationen sowie Kommunikationsdaten aus E-Mails abgesehen. Als Täter nannten die Befragten insbesondere ehemalige Mitarbeiter, Privatpersonen und das unternehmerische Umfeld (also beispielsweise konkurrierende Unternehmen, Lieferanten oder

Kunden). Die in den Medien häufig genannten Angriffe durch ausländische Nachrichtendienste oder organisierte Hacker spielen eine vergleichsweise geringe Rolle.

Eine neue Qualität der Angriffe

Die Angriffe mit der Schadsoftware Emotet zeigen, wie weit fortgeschritten die Entwicklung von Schadsoftware bereits ist. Emotet ist komplett modular aufgebaut und in der Lage, Module für bestimmte Angriffe (z.B. das Ausspähen von Zugangsdaten oder das Auslesen von Adressbüchern) bei Bedarf nachzuladen.

Die Infektion der Rechner geschieht mit Makros, die sich in verlinkten oder in einer E-Mail enthaltenen Microsoft-Office- oder PDF-Datei befinden. Jetzt sagen sie natürlich: Wer öffnet denn im Jahr 2019 noch E-Mail mit einer Datei von einem unbekannten Absender?

Leider ist die Vorgehensweise der Schadsoftware nicht so leicht zu durchschauen:[4] Die E-Mail mit der Schadsoftware kommt in der Regel nicht von einem unbekannten Absender, sondern nimmt Bezug auf eine tatsächlich von dem angegriffenen Anwender versandte E-Mail. Sie erhalten also eine Nachricht von Jemandem, der mit ihnen bereits E-Mails ausgetauscht hat und dessen Systeme durch Emotet infiziert sind.

Die Schadsoftware durchsucht die befallenen Systeme auf vorhandene E-Mails und generiert neue Nachrichten, basierend auf den Inhalten der vorhandenen E-Mails. Findet Emotet beispielsweise eine Nachricht mit einer Bestellung, so generiert es eine Antwort auf diese Nachricht in Form einer Bestellbestätigung.

Der Empfänger öffnet die Nachricht und den darin enthaltenen Dateianhang in der Annahme, dass es sich tatsächlich um eine Bestellbestätigung handelt und infiziert damit seinen Rechner. Mit der Infektion durch Emotet können nun die E-Mails dieses Anwenders ausgelesen und weitere Rechner infiziert werden.

Abb.: Colourbox

Infektion durch Schadsoftware stellte laut BSI auch im letzten Jahr wie schon in den Vorjahren die größte Bedrohung für die Informationssicherheit dar.

Darüber hinaus kann Emotet aber noch zusätzliche Schadsoftware aus dem Internet nachladen. Diese durchsucht dann beispielsweise das gesamte Netzwerk, in dem sich der infizierte Rechner befindet und versucht, vorhandene Schwachstellen automatisiert auszunutzen. Sobald eine Schwachstelle gefunden ist kann Emotet jederzeit weitere Funktionalitäten, beispielsweise zur Verschlüsselung der infizierten Systeme, herunterladen und anwenden. In der Regel verschlüsseln die Angreifer die Daten und verlangen Lösegeld für deren Entschlüsselung.

Was tun?

Erfolgreiche Angriffe zeichnen sich durch eine Kombination verschiedener Methoden aus, die es den Tätern ermöglichen, in die Systeme ihrer Opfer einzudringen. Dazu nutzen sie technische, organisatorische und menschliche Schwachstellen aus.

Bei der für Emotet beschriebenen Vorgehensweise hätte eine zentrale Sicherheitslösung (sogenanntes Unified-Thread-Management) Nachrichten mit angehängten Microsoft-Office-Dokumenten ausfiltern können.

Aber: Da der Anwender dem Absender im geschilderten Fall vertraut, besteht eine hohe Wahrscheinlichkeit, dass die Nachricht trotz Dateianhang an den Anwender weitergeleitet wird (weil dieser bei der IT-Abteilung die Unbedenklichkeit der Nachricht bestätigt und um die Weiterleitung bittet). Dann wäre die automatische Ausfilterung der Schadsoftware durch ein manuelles Eingreifen eines Anwenders außer Kraft gesetzt. Und ein vollständiger Verzicht auf das Senden und Empfangen von Dateianhängen wird nur selten realisierbar sein.

Das bedeutet jedoch nicht, dass sie vorhandene technische Sicherheitslösungen abschaffen sollten. Im Gegenteil: Sie können die Informationssicherheit ihrer Or-

ganisation nur dann deutlich verbessern, wenn Sie wissen, welche Risiken zuverlässig automatisiert von vorhandenen technischen Lösungen adressiert werden. Die verbleibenden Risiken müssen sie anschließend bewerten und klassifizieren. Darauf aufbauend entscheiden sie, ob sie zusätzliche technische Maßnahmen implementieren, organisatorische Anpassungen vornehmen oder einzelne Risiken gegebenenfalls auch akzeptieren.

Nach dieser Bestandsaufnahme besteht der nächste Schritt darin, das Bewusstsein für das Thema Informationssicherheit zu verbessern. Wenn Nachfragen zum Thema Informationssicherheit nicht als Belastung, sondern als Möglichkeit zur Verbesserung der gesamten Organisationssicherheit betrachtet werden, ist bereits viel gewonnen.

Gut geschulte Mitarbeiter lassen die Unbedenklichkeit eines Dateianhangs im Zweifelsfall durch den Informationssicherheitsbeauftragten ihrer Organisation technisch überprüfen, bevor sie einen Dateianhang öffnen. Die bereits oben genannte Befragung der Bitkom e.V. führte zu dem Ergebnis, dass Sicherheitsvorfälle insbesondere durch Hinweise der eigenen Mitarbeiter, durch technische Sicherheitsmaßnahmen wie Virenscanner oder Firewall erkannt wurden.

Ergänzen Sie also die internen Maßnahmen durch Unterstützung von außen. Lassen Sie regelmäßig unabhängige Dritte das Thema Informationssicherheit in ihrer Organisation untersuchen. Die IT-Prüfungshandlungen (und die ggf. getroffenen Feststellungen), die Wirtschaftsprüfer regelmäßig im Rahmen der gesetzlichen oder freiwilligen Jahresabschlussprüfung pflichtgemäß durchführen, können eine gute Grundlage für weitere Prüfungen und Maßnahmen zum Thema Informationssicherheit bieten.

Abb.: Colourbox

Erarbeiten Sie in diesem Jahr gemeinsam mit einem idealerweise unabhängigen Dritten eine Vorgehensweise, wie die Informationssicherheit ihrer Organisation verbessert werden kann.

Profitieren Sie von diesen Erkenntnissen und erarbeiten Sie gemeinsam mit einem idealerweise unabhängigen Dritten (z. B. ihrem Wirtschaftsprüfer) eine Vorgehensweise, wie die Informationssicherheit ihrer Organisation verbessert werden kann. Im Hinblick auf die Buchführung ist festzuhalten, dass Informationssicherheit die Grundvoraussetzung für eine ordnungsmäßige Buchführung und somit für die Erteilung eines uneingeschränkten Bestätigungsvermerks für die Jahresabschlussprüfung darstellt.

Fazit

Eine Organisation nutzt Informationstechnologie als Werkzeug, da sie sich mit ihrer Hauptaufgabe anderen Zwecken verschrieben hat. Dennoch stellt in der heutigen Zeit ein Ausfall der IT ein großes Problem dar, welches die Arbeitsfähigkeit einer Organisation hemmt oder gar zum Erliegen bringt. Gelingt es, innerhalb von Organisationen ein Bewusstsein für das Thema Informationssicherheit zu schaffen und das Thema in der Unternehmenskultur auf allen Ebenen (das gilt auch und insbesondere für Führungskräfte) zu verankern, ist bereits viel erreicht.

Wenn dieses Informationssicherheitsbewusstsein mit individuell auf die Organisation abgestimmten technischen und organisatorischen Maßnahmen sowie regelmäßigen externen Prüfungen kombiniert wird, sind sie auch für die Zukunft gut aufgestellt.

Literaturhinweise

[1] https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-100-Milliarden-Euro-Schaden-pro-Jahr.

[2] https://bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf

[3] https://www.bitkom.org/sites/default/files/2019-11/bitkom_wirtschaftsschutz_2019_0.pdf

[4] https://www.heise.de/security/artikel/Emotet-Trickbot-Ryuk-ein-explosiver-Malware-Cocktail-4573848.html