NIS-2 aktiv statt reaktiv umsetzen

Datenwäsche: Cyberangriffe stoppen, bevor sie starten

Die Cyberbedrohungslage in Deutschland verschärft sich kontinuierlich – darin sind sich alle Sicherheitsbehörden einig. Für von NIS-2 betroffene Unternehmen ist es kostengünstiger, IT-Risiken frühzeitig zu vermeiden, als später aufwendige Meldungen und Krisenmanagement zu betreiben. Präventive Maßnahmen werden daher immer wichtiger.

Von Ramon Mörl, itWatch GmbH

Jeder Angriff erfordert ein Stückchen Code, der sich in Daten oder ausführbaren Elementen verbirgt – sei es in Downloads, E-Mails, mobilen Datenträgern, der Firmware angeschlossener Hardware oder sogar in Software-Patches. Es gibt zahlreiche Einfallstore. Daten aus der Personalabteilung (etwa Bewerbungen), dem Vertrieb, dem Kundenservice, dem Marketing oder der Technik sind nicht zwangsläufig so vertrauenswürdig wie interne Unternehmensdaten. Bevor solche Daten intern genutzt werden können, müssen sie überprüft und gesäubert werden. Eine einfache Antivirenprüfung genügt nicht, da selbst infizierte Dateien wertvolle Informationen oder Bewerbungen für die Personalabteilung enthalten können – schließlich schützt nicht jeder Bewerber sein Smartphone ausreichend. Dieser Prozess wird als Datenwäsche bezeichnet.

Durch das Öffnen einer Bilddatei im JPG-Format oder eines PDF-Dokuments kann etwa ein Skript geladen werden, das die Konfiguration des Remote-Desktop-Tools so verändert, dass Unbefugte die Rechte des Mitarbeiters übernehmen können. Schädlich, aber kein bekannter Schadcode. Auch verschlüsselte Daten in Archiven wie ZIP und anderen Formaten oder in beliebigen anderen Dateien können schädliche Objekte bis auf die Clients und Server transportieren – und entgehen dabei gängigen Schutzmechanismen. Bekannte Viren können von Antivirenscannern (AV) nicht erkannt und neutralisiert werden, wenn sie in einer verschlüsselten Datei oder in tief verschachtelten Archiven eingebettet sind.

Schadsoftware, die zum Beispiel versteckt in verschlüsselten E-Mail-Anhängen unbemerkt ins Unternehmen gelangt und sich im gesamten betriebsinternen System ausbreitet, bedroht die eigene kritische IT erheblich. Kritisch ist natürlich auch das Ausbreiten von Schadcode in den Produkten eines Unternehmens, da die gesamte weitere Lieferkette betroffen ist und zudem ein nicht zu

Bild: itWatch/iStock.com

unterschätzendes und oft unklares Haftungsrisiko entsteht. Für KRITIS-Organisationen ist deshalb auch die Prüfung zugelieferter Software- und Hardwareprodukte wesentlich. Leicht kann in einem Rauchmelder, einer Überwachungskamera oder anderen Geräten zusätzliche Funktionalität wie Wi-Fi, Mikrofon und Kamera untergebracht sein und so auch in nicht vernetzten Geräten eine Bedrohung entstehen.

Cybersicherheit als Enabler

In den oben beschriebenen Szenarien ist „Nicht anklicken, nicht öffnen, nicht nutzen“ keine Option! Die kritischen Leistungen und Services müssen in NIS-2 regulierten Organisationen – trotz möglicher Angriffe – erbracht und die damit verbundenen Arbeiten weiter erledigt werden. Dazu muss die IT für diese Arbeiten funktionieren. Eine Netztrennung zwischen kritischen IT-Elementen und weniger sensibler Infrastruktur schützt die KRITIS-Elemente, addiert aber Komplexität und wird oft – wie viele präventive Sicherheitsmaßnahmen – vom Anwender als hinderlich wahrgenommen. Das Problem wird durch eine netztrennende Schleuse mit Datenwäsche

und Workflow nach einem patentierten Verfahren gelöst (itWash.de). Diese netztrennende Datenschleuse ist auch gegenüber dem Internet bezüglich E-Mails aus unsicheren Domänen, Downloads oder Datentransportverfahren wie OneDrive, WeTransfer, S-FTP nutzbar.

Jeder unbekannte Code im Datenzufluss von extern nach intern wird identifiziert. Datenobjekte dürfen nur bekannte oder vertrauenswürdige Codeelemente enthalten – signierte Skripte, Makros oder solche, die in einer Whitelist mit ihren authentisierenden Eigenschaften hinterlegt sind.

Eingehender Code, also neue Software, Patches et cetera, wird nur von einem vertrauenswürdigen Kanal übernommen und in seine Bestandteile zerlegt, indem eine Software Bill of Material (SBOM) erstellt wird. Zu jedem Element werden die Verletzbarkeiten (Common Vulnerabilities and Exposures, CVE) ermittelt und für das Lifecyclemanagement hinterlegt. Die Betriebssystemhärtung durch die itWatch Enterprise Security Suite (itWESS.de) übernimmt die freigegebenen Softwareelemente in ihre Whitelist. Die CVEs werden zyklisch neu geprüft und bei definierten Schwellwerten geeignet reagiert (Alert oder Sperre).

Datenwäsche mit passendem Waschpulver

Die Datenwäsche besteht darin, die Daten in ihre Einzelteile zu zerlegen und jedes einzelne Element rekursiv einzeln erneut der Wäsche zuzuführen. Für jeden Datentyp wird automatisch das richtige Waschprogramm und Waschpulver gewählt. Danach werden die sauberen, also von allem Schmutz befreiten Daten, wieder zusammengesetzt und der Anwender erhält einen Bericht, ob und was verändert wurde. Schmutzige Elemente werden zur Beweissicherung gespeichert – natürlich verschlüsselt, damit sie nicht „ausbrechen“ können.

Die Voraussetzung für eine Wäsche ist, dass die Daten im Klartext vorliegen – denn eine Wäsche in einer wasserdicht verschlossenen Verpackung würde auch in der analogen Welt keinen Sinn ergeben. itWash verfügt deshalb über eine Erkennung von verschlüsselten Objekten und führt diese vor der Wäsche der Entschlüsselung durch den Anwender zu, ohne dass dessen Betriebssystem auf die Daten zugreifen kann.

Ein wesentlicher Vorteil gegenüber anderen Verfahren ist, dass jeder Bestandteil rekursiv zerlegt wird und jedes einzelne entstehende Objekt erneut allen Prüfungen – Verschlüsselung, Antivirus, Dateitypenauthentisierung, Inhaltsprüfung et cetera – unterzogen wird. Hierbei werden Verschlüsselungen und Modifikationen sicher erkannt und berücksichtigt. Insofern sind die in itWash angewendeten Verfahren deutlich mächtiger als die unter Content Disarm and Recover (CDR) vermarkteten Lösungen und können genauso auf dem Weg „nach draußen“ als Data Loss Prevention (DLP) eingesetzt werden.

Während der Wäsche werden automatisch Informationen zur richtigen Behandlung gewonnen – darunter der Einlieferer, die Herkunft sowie enthaltene Metadaten wie Geolokationen, Zeitstempel, erkannte Objekte in Bildern oder transkribierter Text aus Sprachdateien (Voice2Text). Diese Daten bestimmen das passende „Waschmittel“, die gewünschte Standardisierung (z. B. Konvertierung von Mediendaten in MP3 oder MP4) und das Ziel, an das die bereinigten Daten weitergeleitet werden sollen. Ein Algorithmus ermittelt das Übertragungsziel, setzt dort die passenden Zugriffsrechte und wendet bei Bedarf die geeignete Verschlüsselung an.

Wenn die eigene IT nicht verändert werden soll oder darf, ist eine Wäsche auch als Service in der Cloud oder in einem Rechenzentrum möglich (siehe Testbeispiel unten). Datenwäsche als mandantenfähiger Managed Service, der sowohl die Datenschutz-Grundverordnung (DSGVO) als auch branchenspezifische Regulierungen erfüllt, kann ganze Unternehmensverbünde und Lieferketten absichern. Weitere Informationen dazu finden Sie im Artikel „Datenwäsche als Cloud-Service“ im <kes>-Special 06/2024.

Security „Made in Germany“

itWatch ist einer der wenigen inhabergeführten Cybersecurity-Hersteller in Deutschland und entwickelt patentierte IT-Sicherheitslösungen „Made in Germany“. Die Enterprise Security Suite (itWESS) und die Datenschleuse (itWash) schützen Tausende als GEHEIM klassifizierte IT-Umgebungen, die auf der Skala der Common-Criteria-Prüfungen höher als eine CC EAL 4+-Prüfung zu bewerten sind, da nicht nur anhand eines herstellerdefinierten Protection-Profiles geprüft wird. Stattdessen werden alle Facetten der Produkte in realen, vernetzten Einsatzumgebungen getestet und durch professionelle Pentester verschiedenen Angriffsszenarien ausgesetzt. ■