Hausarbeit: Analyse aktueller Cyberangriffe und Sicherheitsmaßnahmen

1. Aktueller Angriff: Die Ransomware-Attacke auf die English Construction Company

Im November 2024 wurde die English Construction Company, ein Bauunternehmen mit Sitz in Lynchburg, Virginia, Ziel eines Ransomware-Angriffs. Der Angriff wurde durch eine initiale Kompromittierung des IT-Systems ermöglicht, bei der Angreifer Zugang zu mehreren Servern erlangten. Diese verschlüsselten die dort gespeicherten Daten und exfiltrierten sensible Informationen, darunter persönliche Daten ehemaliger Mitarbeiter wie Namen, Sozialversicherungsnummern, Adressen, Führerscheinnummern und Geburtsdaten.

Die Angreifer nutzten vermutlich Phishing-E-Mails oder andere Techniken, um sich Zugang zu verschaffen, bevor sie die Ransomware einsetzten. Nach der Entdeckung des Vorfalls isolierte das Unternehmen die betroffenen Systeme und beauftragte externe Cybersicherheits-Experten mit der Untersuchung und Behebung des Problems. Dennoch war ein signifikanter Datenverlust unvermeidbar. Dieser Fall unterstreicht die Wichtigkeit robuster Sicherheitsstrategien, regelmäßiger Sicherheitsupdates und einer schnellen Reaktionsfähigkeit auf Sicherheitsvorfälle.

- https://www.jdsupra.com/legalnews/english-construction-company-targeted-8647430/

2. Bekannte Schwachstellen in SOGo Web Mail 2023

CVE-ID	Beschreibung	Betroffene Versionen	Schweregrad (CVSS)	Lösung
CVE-2023-48104	HTML-Injection ermöglicht es Angreifern, schädliche Inhalte in E-Mails einzufügen und Benutzerdaten abzufangen.	SOGo Web Mail < 5.9.1	Mittel (6.1)	Update auf Version 5.9.1 oder höher, um die HTML-Injection durch Validierung der Eingaben zu verhindern.
CVE-2020-22402	XSS (Cross-Site Scripting) erlaubt Angreifern den Diebstahl sensibler Informationen durch schädliche E-Mails.	SOGo Web Mail < 4.3.1	Mittel (6.1)	Aktualisierung auf mindestens Version 4.3.1 erforderlich.

Die National Vulnerability Database (NVD) listet mehrere Schwachstellen in der Webmail-Software SOGo, die 2023 entdeckt wurden. Eine bedeutende Schwachstelle ist **CVE-2023-29540**, die es Angreifern ermöglicht, einen Denial-of-Service (DoS) herbeizuführen. Eine weitere Schwachstelle, **CVE-2023-31824**, betrifft unzureichende Authentifizierungsmechanismen an API-Endpunkten, wodurch unbefugte Zugriffe auf sensible Benutzerdaten möglich sind.

Zur Behebung solcher Schwachstellen sollten Entwickler entsprechende Patches bereitstellen, während Benutzer sicherstellen müssen, dass ihre Systeme stets auf dem neuesten Stand sind. Zusätzliche Maßnahmen

wie die Aktivierung von Multi-Faktor-Authentifizierung und das Einschränken von Berechtigungen können ebenfalls dazu beitragen, die Sicherheit zu erhöhen.

Hinweise:

- **CVE-2023-48104** ist besonders relevant für Phishing-Angriffe, da bösartige Formulare in den E-Mail-Inhalt eingebettet werden können. Die Behebung erfolgte durch striktere Eingabevalidierung in neueren Versionen.
- **CVE-2020-22402** wurde zwar früher entdeckt, ist aber in den NVD-Daten für 2023 weiterhin aufgeführt, da ältere Systeme potenziell verwundbar bleiben.

Aufgabe 3: Application Whitelisting mit WDAC

Überarbeitete Antwort: Aufgabe 3 – Application Whitelisting mit WDAC

1. Wie funktioniert Application Whitelisting mit WDAC und wie unterscheidet es sich von AppLocker?

Windows Defender Application Control (WDAC) ermöglicht die Erstellung von Sicherheitsrichtlinien, die festlegen, welche Anwendungen und Skripte auf einem System ausgeführt werden dürfen. WDAC arbeitet auf Kernel-Ebene und verwendet kryptografische Signaturen oder Hash-Werte, um die Integrität von Anwendungen zu überprüfen.

AppLocker hingegen ist ein weniger komplexes Whitelisting-Tool, das auf Gruppenrichtlinien basiert. Es bietet ebenfalls Richtlinien für die Steuerung der Softwareausführung, ist jedoch einfacher zu konfigurieren und wird häufig in weniger sicherheitskritischen Umgebungen eingesetzt.

Hauptunterschiede:

- **WDAC**: Für Umgebungen mit hohen Sicherheitsanforderungen, arbeitet auf Kernel-Ebene, tiefergehende Kontrolle, granularere Richtlinien.
- **AppLocker**: Für kleinere Unternehmen oder weniger komplexe Szenarien, einfacher zu implementieren, aber weniger tiefgreifend.

2. Wie schränkt WDAC Benutzer/Prozesse bei der Codeausführung ein?

WDAC erzwingt strenge Richtlinien, die nur signierten oder explizit genehmigten Anwendungen und Skripten die Ausführung erlauben. Die Verifikation erfolgt über:

- **Signaturen**: Überprüfung der digitalen Signatur.
- **Hash-Werte**: Abgleich mit vordefinierten Hashes in der Richtlinie.

Selbst Administratoren können keine nicht genehmigten Anwendungen ausführen, was Systeme effektiv vor unautorisiertem Code schützt, einschließlich Zero-Day-Exploits und Malware.

3. Wie schränkt WDAC Benutzer/Prozesse beim Lesen von Dateien ein?

WDAC steuert keine direkten Datei-Lesezugriffe.
Es kontrolliert ausschließlich, welche Anwendungen ausgeführt werden dürfen. Dadurch wird indirekt verhindert, dass nicht autorisierte Programme schädliche Dateien oder Daten lesen und verarbeiten können.

4. Wie schränkt WDAC Benutzer/Prozesse beim Schreiben von Dateien ein?

WDAC regelt keine direkten Datei-Schreibzugriffe.
Die Richtlinien verhindern jedoch, dass nicht autorisierte Anwendungen gestartet werden. Dadurch wird das Risiko reduziert, dass Malware bösartigen Code ins System schreibt oder persistente Bedrohungen erstellt.

5. Welche Dateiregeln können Sie mit WDAC verwenden?

1. **Hash**: Regeln basieren auf den spezifischen Hash-Werten von Binärdateien. Änderungen an der Datei erfordern ein Update der Richtlinie.
2. **FileName**: Basierend auf dem Namen der Datei (z. B. `OriginalFileName`). Weniger sicher, aber einfacher zu verwalten.
3. **FilePath**: Erlaubt die Ausführung von Binärdateien aus definierten Verzeichnissen (gilt nur im Benutzer-Modus).
4. **SignedVersion**: Erlaubt signierte Anwendungen eines Herausgebers mit einer Mindestversionsnummer.
5. **Publisher**: Vertrauenswürdigkeit basierend auf dem Herausgeber der Anwendung.
6. **FilePublisher**: Kombiniert Herausgeberinformationen, Dateinamen und Mindestversion.
7. **LeafCertificate**: Basierend auf einem spezifischen Signaturzertifikat.
8. **PcaCertificate**: Vertrauenswürdigkeit für Zertifikate eine Ebene unterhalb des Root-Zertifikats.
9. **WHQL**: Unterstützt von Microsoft zertifizierte Treiber (Windows Hardware Quality Labs).
10. **WHQLPublisher/WHQLFilePublisher**: Kombination aus WHQL-Zertifizierung und Herausgeberregeln, insbesondere für Kernel-Treiber.

6. Was ist der Zweck des Audit-Modus in WDAC?

Der **Audit-Modus** ermöglicht die Evaluierung von WDAC-Richtlinien, ohne die Ausführung von Anwendungen tatsächlich zu blockieren. Dabei werden alle Verstöße protokolliert, sodass Administratoren die Richtlinien anpassen können, bevor sie in den Erzwingungsmodus wechseln. Dies minimiert Betriebsunterbrechungen und erleichtert die Einführung neuer Richtlinien.

7. Wie debuggen Sie WDAC-Richtlinien? Welche Logging-Ressourcen können genutzt werden?

1. **Ereignisanzeige (Event Viewer):**
   - Protokoll: `Microsoft-Windows-CodeIntegrity/Operational`.
   - Enthält detaillierte Informationen zu blockierten Anwendungen und deren Gründen.
2. **PowerShell:**
   - Cmdlets wie `Get-WinEvent` zur Analyse spezifischer WDAC-Ereignisse.
3. **Microsoft Defender Advanced Threat Protection (ATP):**
   - Detaillierte Berichte über blockierte Anwendungen und potenzielle Richtlinienkonflikte.
4. **PolicyAnalyzer:**
   - Ein Microsoft-Tool zur Analyse und Optimierung von WDAC-Richtlinien.
5. **Weitere Ressourcen:**

- Debugging-Logs mit Hilfe von `ConvertFrom-CIPolicy` und `Merge-CIPolicy`, um Richtlinienänderungen zu überprüfen.