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

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

WDAC basiert auf der Definition von Sicherheitsrichtlinien, die festlegen, welche Anwendungen und Skripte auf einem System ausgeführt werden dürfen. Es arbeitet tief auf Kernel-Ebene und verwendet kryptografische Signaturen oder Hash-Werte, um Anwendungen zu verifizieren.

AppLocker, ein anderes Tool für Application Whitelisting, bietet ebenfalls Richtlinien zur Steuerung von Softwareausführung, ist jedoch benutzerfreundlicher und weniger tiefgreifend. Der Hauptunterschied liegt in der Zielgruppe und Funktionsweise:

- **WDAC**: Für hochsichere Umgebungen, mit granularen Richtlinien und tiefgreifender Kontrolle.
- **AppLocker**: Geeignet für kleinere Unternehmen oder weniger komplexe Umgebungen, einfacher zu konfigurieren und zu verwalten.

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

WDAC erlaubt die Ausführung von Code nur, wenn dieser mit einer genehmigten Signatur oder einem Hash-Wert übereinstimmt. Nicht genehmigte Software wird blockiert, auch wenn sie von Administratoren ausgeführt wird. Dies schützt Systeme effektiv vor Zero-Day-Exploits und nicht autorisierten Anwendungen.

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

WDAC konzentriert sich primär auf die Kontrolle der Codeausführung und bietet keine direkte Steuerung des Lesens von Dateien. Indirekt schützt es jedoch vor dem Lesen und Ausführen schädlicher Skripte, indem es nur vertrauenswürdigen Anwendungen den Zugriff auf Systemressourcen erlaubt.

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

WDAC beschränkt das Schreiben von Dateien nicht direkt, sondern verhindert, dass nicht autorisierte Anwendungen Code schreiben oder installieren. Dies reduziert das Risiko, dass Malware bösartigen Code ins System injiziert.

5. Welche Dateiregeln können Sie mit WDAC verwenden?

1. **Hash**: Sehr spezifisch, basiert auf den Hash-Werten der Binärdateien. Erfordert häufige Updates bei Versionänderungen.

2. **FileName**: Nutzt Dateinamen (*z. B. OriginalFileName*). Weniger sicher, aber minimiert Richtlinienaktualisierungen.
3. **FilePath**: Erlaubt Binärdateien aus bestimmten Dateipfaden (nur Benutzer-Modus).
4. **SignedVersion**: Erlaubt Binärdateien von bestimmten Herausgebern mit Mindestversionsnummern.
5. **Publisher**: Vertrauenswürdig für Dateien eines spezifischen Herausgebers (z. B. Intel).
6. **FilePublisher**: Kombiniert Dateinamen, Herausgeber und Mindestversion für spezifische signierte Dateien.
7. **LeafCertificate**: Vertrauenswürdig für spezifische Signaturzertifikate; Updates nur bei Ablauf erforderlich.
8. **PcaCertificate**: Vertrauenswürdigkeit für Zertifikate eine Stufe unterhalb des Root-Zertifikats.
9. **WHQL**: Unterstützt von Microsoft zertifizierte Treiber (WHQL).
10. **WHQLPublisher/WHQLFilePublisher**: Kombiniert WHQL mit Herausgeber- oder Dateinamenregeln, hauptsächlich für Kernel-Treiber.

- https://learn.microsoft.com/en-us/windows/security/application-security/application-control/app-control-for-business/design/select-types-of-rules-to-create

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

Der Audit-Modus dient zur Testung von WDAC-Richtlinien, ohne die Ausführung von Anwendungen tatsächlich zu blockieren. Administratoren können damit potenzielle Probleme oder Konflikte identifizieren und sicherstellen, dass die Richtlinien wie gewünscht funktionieren, bevor sie durchgesetzt werden.

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

- **Ereignisanzeige (Event Viewer)**: Speichert alle Aktivitäten und Blockierungen im Protokoll „Microsoft-Windows-CodeIntegrity/Operational“.
- **PowerShell**: Cmdlets wie `Get-WinEvent` helfen bei der Abfrage spezifischer Ereignisse.
- **Microsoft Defender Advanced Threat Protection**: Bietet detaillierte Einblicke in Richtlinienwirkungen.
- **Spezifische Tools**: Anwendungen wie `PolicyAnalyzer` analysieren WDAC-Richtlinien und erkennen mögliche Lücken oder Fehler.