FORENOVA

Bericht über die Verwaltung externer Angriffsflächen (EASM)

Beispiel Real Estate GmbH

Durchgeführtes Datum: April 4, 2025

Projekthintergrund

Das Sicherheitsteam von ForeNova wurde von Example Real Estate Gmbh beauftragt, am 4. April 2025 eine umfassende Bewertung des External Attack Surface Management (EASM) durchzuführen. Der Umfang umfasste:

- Analyse der Internetbelastung
- Aufdeckung externer Angriffsflächen

Name des Kunden: XX Real Estate GmbH
Überwachte Domains: *(Aus Gründen der Vertraulichkeit geschwärzt; siehe Anhang)*
IP-Segmente: 111.***.***.65/28, 8.***.***.225, 124.***.***.96/27, 124.***.***.237/30

Zusammenfassung

Es wurden insgesamt 48 Subdomain-Assets, 353 Webseiten und 47 digitale Assets identifiziert. Kritische Schwachstellen wie Remote Code Execution (RCE) und SQL Injection waren vorhanden und stellten ein hohes Risiko für das Unternehmen dar.

Die wichtigsten Probleme sind:

- Gefährdung sensibler Dokumente
- Impersonation von Websites
- Öffentlich zugängliche Backend-Anmeldeportale
- SQL-Injection in Verwaltungsschnittstellen
- Unsichere Konfigurationen auf öffentlichen IPs

Überblick über die Internetpräsenz

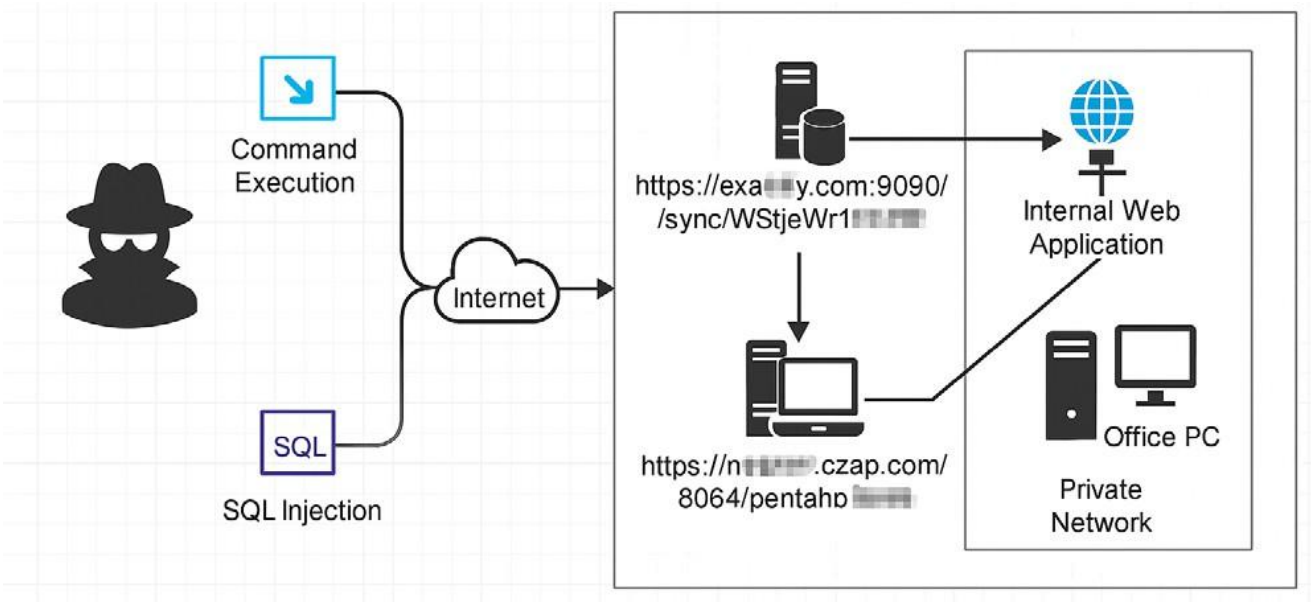
Asset-Typ	Anzahl
Root-Domain-Namen	2
Subdomain Assets	48
IP-Adressen	54
Offene Ports	633
Webdienste	353
Nicht-Web-Vermögenswerte	280
Cloud Assets	22
SSL-Zertifikate	13

Externe Risiken Zusammenfassung

Risiko Typ	Hoch	Mittel	Niedrig
Schwachstellen	11	18	1
Schwache Passwörter	0	0	0
Wesentliche Komponenten	37	-	-
Ports/Dienst Expositionen	8	-	-

Angriffsvektoren

Karte der Angriffsroute



Details zum Angriff

Angreifer können Schwachstellen wie SQL-Injection oder Befehlsausführung in öffentlich zugänglichen Systemen ausnutzen, um:

- Unbefugten Zugriff zu erhalte
- Privilegien zu erweitern
- sich seitlich in internen Netzwerken zu bewegen

Seitliche Bewegung Methoden:

- Sammeln von Zugangsdaten von kompromittierten Servern
- Ausnutzen bekannter Schwachstellen (z.B. MS17-010)
- Brute-Force-Angriffe auf interne Anmeldesysteme

Domain-Namen

Beispiel-Domains (vollständige Liste geschwärzt):

- xfw.m***y.com
- tjs***m.m***y.com
- sjz***nchant.m***y.com
- mail.m***y.com
- vpn.m***y.com

IP-Adressen

Probenbereich:

- 111.***.***.65 – 111.***.***.77

Hochrisikobehaftete Vermögenswerte

Gastgeber	Hafen	Service
sjbi.my.com	3389	RDP
111.*..130	6379	Redis
111.*..152	5985	WinRM
8.*..225	3389	RDP

Offene Ports und Dienste

Gastgeber	Hafen	URL	Technologie Stack
www.m***y.com	1187	http://www.m***y.com:1187	PHP, jQuery, nginx, Tongda OA
mail.m***y.com	80	http://mail.m***y.com	Apache httpd
124.*..109	8088	http://124.***.**.109:8088	Panmicro e-Bridge, nginx

Detailliertes Beispiel für eine Schwachstelle

SQL-Einschleusung (kritisch)

URL

https://sj***portal.m***y.com:9070/system/adminUsers/getAdminUsersList.do?state=1

Risiko: Ermöglicht Angreifern, bösartige SQL-Abfragen einzuschleusen, um die Authentifizierung zu umgehen oder auf sensible Daten zuzugreifen.

Proof-of-Concept Schnipsel:

POST /system/adminUsers/getAdminUsersList.do?state=1 HTTP/1.1

Einspritzung in: sortName=(case when 1=1 then name else id end)

Empfehlungen:

- Erzwingen Sie eine strenge Eingabevalidierung
- Implementieren Sie parametrisierte Abfragen
- Schränken Sie die Zugriffsrechte für Datenbanken ein
- Setzen Sie WAFs mit SQLi-Erkennung ein

Hochrangige Empfehlungen

Beheben Sie kritische Schwachstellen

Patchen Sie Systeme, die von SQL Injection und Remote Code Execution (RCE) betroffen sind.

- Reinigen Sie alle Benutzereingaben (verwenden Sie Whitelisting und Eingabevalidierung).
- Verwenden Sie parametrisierte SQL-Abfragen in allen Anwendungen.
- Patchen Sie anfällige Systeme und aktualisieren Sie Frameworks.
- Setzen Sie eine Web Application Firewall (WAF) mit SQLi/RCE-Schutz ein

Beschränken Sie den öffentlichen Zugang zu sensiblen Diensten

Sperren Sie Dienste wie RDP, WinRM, Redis und Verwaltungsportale.

- Verwenden Sie Firewall-Regeln, um den Zugriff auf bestimmte IPs zu beschränken.
- Erzwingen Sie den VPN-Zugang für die Fernverwaltung.
- Deaktivieren Sie ungenutzte Dienste oder verschieben Sie sie hinter Authentifizierungs-Gateways.

Entfernen oder sichern Sie freiliegende Dokumente

Identifizieren und entfernen Sie online veröffentlichte Dokumente.

- Verwenden Sie Tools wie Google Dorking oder DLP-Scanner, um exponierte Dokumente zu finden.
- Überprüfen Sie öffentliche Ordner oder falsch konfigurierte Cloud-Buckets.
- Legen Sie die richtigen Dateiberechtigungen fest und verschlüsseln Sie sensible Dateien.

Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA)

Fügen Sie MFA zu allen nach außen gerichteten Portalen und Benutzerkonten hinzu.

- Verwenden Sie App-basierte MFA (wie Google Authenticator oder Microsoft Authenticator).
- Erzwingen Sie MFA für E-Mail, VPN, Admin-Dashboards und Cloud-Konten.
- Informieren Sie die Benutzer über phishing-sichere MFA.

Bereitstellen einer Web Application Firewall (WAF)

Verwenden Sie eine WAF, um Webanwendungen vor gängigen Angriffen zu schützen.

- Wählen Sie eine WAF (z.B. Cloudflare, AWS WAF oder Imperva).
- Legen Sie Regeln fest, um bösartigen Datenverkehr zu blockieren.
- Überwachen Sie Protokolle und Warnmeldungen, um blockierte Bedrohungen zu verfolgen.

Überwachen und bereinigen Sie gefährdete Vermögenswerte

Entdecken und sichern Sie kontinuierlich exponierte Domains, Subdomains und Dienste.

- Verwenden Sie EASM-Tools (z.B. Shodan, Censys oder Attack Surface Management Plattformen).
- Prüfen Sie DNS-Einträge und IP-Bereiche monatlich.
- Entfernen oder deaktivieren Sie veraltete Subdomänen und Assets.

Härten Sie öffentlich zugängliche Dienste

Sichere Dienste wie Webmail, VPNs und Portale.

- Deaktivieren Sie Standardkonten oder ändern Sie Standardkennwörter.
- Deaktivieren Sie Verzeichniseinträge und unnötige Funktionen.
- Verwenden Sie sichere Protokolle (HTTPS, SFTP, usw.).