MYRA

THREAT ASSESSMENT CARD

Welche Bedrohungen Ihre Anwendungs- und Netzwerksicherheit gefährden

Threat Assessment Card

Welche Bedrohungen Ihre Anwendungs- und Netzwerksicherheit gefährden

Unternehmen aller Branchen und Behörden sehen sich einer Vielzahl von Online-Bedrohungen ausgesetzt. Cyberkriminelle attackieren zum Beispiel gezielt Webseiten, Webapplikationen, Online-Schnittstellen (APIs) und IT-Infrastrukturen mittels DDoS-Angriffen, um digitale Geschäftsprozesse zu stören und möglichst viel Schaden anzurichten. Außerdem zielen Bedrohungsakteure mit unterschiedlichsten Angriffstechniken darauf ab, Zugänge zu kompromittieren und anschließend Daten zu stehlen, zu manipulieren oder auszuspionieren.

Die folgende Übersicht führt die häufigsten Bedrohungen für Webanwendungen und IT-Infrastrukturen auf. Anhand der Liste können Sie die Risiken einschätzen (kein Risiko, niedrig, mittel, hoch), denen Ihr Unternehmen oder Ihre Institution ausgesetzt ist. So erhalten Sie schnell und einfach ein Bild Ihrer individuellen Bedrohungslage, das Ihnen dabei hilft, geeignete Schutzmaßnahmen zu identifizieren.

Angriffsrisiko	kein Risiko	niedrig	mittel	hoch	DSGVO-konforme Lösung im Einsatz
Ausfall (Website, Apps, APIs) durch					
DDoS Layer 3/4	☐	☐	☐	☐	☐
DDoS Layer 7	☐	☐	☐	☐	☐
Lastspitzen	☐	☐	☐	☐	☐
abgelaufenes SSL/TLS-Zertifikat	☐	☐	☐	☐	☐
Datendiebstahl durch					
Account Takeover	☐	☐	☐	☐	☐
Cross-Site Scripting (XSS)	☐	☐	☐	☐	☐
Cross-Site Request Forgery (CSRF)	☐	☐	☐	☐	☐
SQL Injection	☐	☐	☐	☐	☐
Manipulation durch					
Form Spam	☐	☐	☐	☐	☐
Hype Sales Bots	☐	☐	☐	☐	☐
Cart Abandonment / Inventory Hoarding	☐	☐	☐	☐	☐
Account Creation	☐	☐	☐	☐	☐
Klickbetrug	☐	☐	☐	☐	☐
Skewing	☐	☐	☐	☐	☐
DNS Cache Poisoning	☐	☐	☐	☐	☐
DNS Spoofing	☐	☐	☐	☐	☐
Spionage durch					
Price Grabbing	☐	☐	☐	☐	☐
Content/Product Grabbing (Web Scraping)	☐	☐	☐	☐	☐
Unautorisierter Zugriff durch					
Credential Stuffing	☐	☐	☐	☐	☐
Credential Cracking	☐	☐	☐	☐	☐
Brute-Force-Attacken	☐	☐	☐	☐	☐

Sie haben ein mittleres bis hohes Angriffsrisiko für Ihre Webseiten, Webapplikationen, Online-Schnittstellen oder IT-Infrastruktur ermittelt? Dann kontaktieren Sie uns via E-Mail (info@myrasecurity.com) oder Telefon (+49 89 414141 – 345) für eine unverbindliche kostenlose Schutzberatung.

Glossar

DDoS Layer 3/4

Angreifer belasten Ihre IT-Infrastruktur mit sehr hohem Traffic-volumen oder immensen Paketraten, um Systemressourcen oder Netzwerkbandbreiten zu überlasten.

DDoS Layer 7

Angreifer senden eine Flut automatisierter Anfragen an Ihren Webserver, um diesen zu überlasten und die darauf gehosteten Seiten oder Dienste lahmzulegen.

Account Creation & Takeover

Bots erstellen massenhaft gefälschte Nutzerkonten oder infiltrieren bestehende Accounts, die Kriminelle anschließend für Angriffe oder Betrugsversuche missbrauchen.

Cross-Site Scripting (XSS)

Bei einem XSS-Angriff injizieren Cyberkriminelle durch Aus-nutzen von Sicherheitslücken schädlichen Code in Webanwen-dungen, um etwa sensible Informationen zu stehlen.

Cross-Site Request Forgery (CSRF)

Angreifer bringen den Browser des Nutzers oder der Nutzerin dazu, HTTP-Requests an die angegriffene Website oder Webapplikation zu schicken, um unerwünschte Aktionen auszulösen.

SQL Injection

Angreifer nutzen gezielt Sicherheitslücken aus, um beispiels-weise über Eingabemasken eigene Befehle und Schadcode in Onlinedienste einzuschleusen, welche die Datenbanksprache SQL verwenden. Auf diese Weise gelangen sie an wertvolle Datensätze oder können Datenbankeinträge manipulieren.

Form Spam

Über Kontaktformulare bombardieren Bots Ihr Unternehmen mit Botschaften. Diese Phishing-Methode dient Kriminellen häufig als Ausgangspunkt für weiterführende Angriffe.

Hype Sales Bots

Durch automatisierte Bot-Anfragen sichern sich Betrüger begehrte Waren und verkaufen sie anschließend mit hohem Gewinn weiter, was sich negativ auf Ihre Kundenbeziehung auswirkt.

Cart Abandonment / Inventory Hoarding

Bots füllen Warenkörbe, ohne den Kaufprozess abzuschließen. Das ist geschäftsschädigend für Ihren Shop, weil reguläre Kund:innen die Artikel temporär nicht mehr kaufen können.

Klickbetrug

Angreifer setzen Bots dazu ein, auf Websites enthaltene Werbeanzeigen oder Affiliate-Links automatisiert anzuklicken, um auf Kosten der Werbetreibenden Einnahmen zu generieren

Skewing

Durch Bot-basierte Anfragen manipulieren Angreifer gezielt Web-Analysedaten, um Sie zu falschen strategischen Entscheidungen zu verleiten und Ihnen zu schaden.

DNS Cache Poisoning

Angreifer schmuggeln verfälschte Einträge in den DNS Cache von Nameservern, um die Zuordnung zwischen Domainnamen und der dazugehörigen IP-Adresse zu manipulieren und User auf gefälschte Webseiten umzuleiten.

DNS Spoofing

Kriminelle manipulieren gezielt DNS-Einträge auf Servern, Routern, PCs oder Mobilgeräten, um User auf andere Webseiten mit meist schädlichen Inhalten umzuleiten. Solche Angriffe zielen etwa darauf ab, wertvolle Login-Daten per Phishing abzugreifen, Schadsoftware zu verbreiten oder Einnahmen durch Klickbetrug zu generieren.

Price Grabbing

Bots spähen Produktpreise oder ganze Preisgefüge aus. Wettbewerber können diese Daten nutzen, um die Preise der Konkurrenz automatisch zu unterbieten.

Content/Product Grabbing

Bots kopieren in Sekundenschnelle einzelne Seiteninhalte oder ganze Websites. Kriminelle nutzen eine solche Kopie der Originalseite, um per Phishing Anmeldedaten abzugreifen.

Credential Stuffing

Bots können in kürzester Zeit massenhaft Nutzer/Passwort-Kombinationen testen. Treffer zu aktiven Accounts werden anschließend verkauft oder für weitere Attacken genutzt.

Credential Cracking

Anders als beim Credential Stuffing sind Angreifern beim Credential Cracking die Zugangsdaten noch nicht gänzlich bekannt. Sie kennen etwa nur den Nutzernamen, aber nicht das Passwort. Daher lassen sie Passwortlisten von Bots automatisiert abarbeiten, bis sie das passende Kennwort gefunden haben.

Brute-Force-Attacken

Brute-Force-Attacken setzen auf leistungsstarke Computer-systeme sowie Tools, die in Kombination automatisierte Anmeldeversuche mit möglichst vielen Nutzer/Passwort-Kombinationen erlauben, um Zugangsdaten zu erhalten.

MYRA
Neue digitale Sicherheit

Made in Germany

Alle Vorteile auf einen Blick

- **Zukunftssichere Technologie:** Vollautomatisiert, hochperformant, selbstlernend und hochskalierbar
- **Hochzertifizierte Qualität:** ISO 27001 auf Basis von IT-Grundschutz, BSI-KRITIS-qualifiziert, BSI-C5-Testat Typ 2, DIN-EN-50600-zertifizierte Rechenzentren, PCI-DSS-zertifiziert, IDW PS 951 Typ 2 (ISAE 3402) geprüft, Trusted Cloud
- **KRITIS-Cluster:** DSGVO-konforme, mehrfach georedundante Server-Infrastruktur in Deutschland
- **Erfahrung:** Myra schützt seit Jahren erfolgreich kritische Infrastrukturen und sensible Sektoren
- **Kostentransparenz:** Keine Mehrkosten im Angriffsfall, justierbare Subscriptions, 100% Planbarkeit
- **Made in Germany:** Technische Kontrolle, stetige Weiterentwicklung, 24/7 Support aus München

Hochzertifizierter Schutz für sensible und regulierte Sektoren

Myra für Finance:
Mit unserem Know-how, unseren smarten Lösungen und umfangreichen Zertifizierungen erfüllen wir seit Jahren für viele namhafte Kunden aus der Finanzbranche die Bedürfnisse nach Cybersicherheit und Compliance. Wir sind Ihr Compliance-Garant für wesentliche und unwesentliche Auslagerungen.

Myra für Health:
Wir haben langjährige Erfahrung in der digitalen Absicherung des Gesundheitsbereichs. Unter anderem schützen wir die Online-Portale des Bundesgesundheitsministeriums, der Bundeszentrale für gesundheitliche Aufklärung (BZgA) sowie diverser Länderbehörden und (Kranken-)Versicherungen.

Myra für Government:
Wir schützen über 500 Domains der Bundesregierung, von Ministerien sowie deutschen Bundes- und Landesbehörden vor Cyberangriffen und Überlastung. Auch bei unvorhersehbaren Lastspitzen sichern wir die Verfügbarkeit von Informationsportalen und Webanwendungen, so dass Millionen Bürger:innen jederzeit darauf zugreifen können.

Myra für KRITIS:
Als kompetenter Partner für KRITIS-Betreiber sichern wir die digitalen Geschäftsprozesse systemkritischer Institutionen zuverlässig ab. Ausfälle hätten hier schwerwiegende Folgen für die Bevölkerung. Dank hochperformanter Technologie und hochzertifizierter Qualität bietet Myra zuverlässigen Schutz in diesem sensiblen Bereich.

Myra für E-Commerce:
Unsere Technologie harmoniert perfekt mit den Anforderungen im Onlinehandel: maximale Performance, niedrige Latenzen und höchste Skalierbarkeit. Wer gegen Amazon, eBay und Co bestehen will, darf sich keine Fehler leisten. Myra sorgt für eine performante Content-Auslieferung und filtert schädliche Abfragen, bevor diese die Kundenserver belasten.

Myra ist der Spezialanbieter für Kunden aus hochregulierten Bereichen

Bundesministerium für Gesundheit · ITSG · msc Munich Security Conference · Barmenia Einfach. Menschlich. · DSV IT Service · Liechtensteinische Landesbank 1861 · BZgA Bundeszentrale für gesundheitliche Aufklärung · flatex DEGIRO

Myra Security GmbH | **Tel. +49 89 414141 – 345** | **www.myrasecurity.com** | **info@myrasecurity.com**