INGRAM MICRO SECURITY

CATALOGUE OVERVIEW

Offensive Security Services

Contents

Einleitung

Die Cybersicherheitsgefahren nehmen stetig zu und alle Unternehmen und Organisationen, unabhängig der Größe, der Branche oder des Standorts, werden von Cyberkriminellen aus aller Welt ins Visier genommen.

Unsere Offensive Security Services sind ein proaktiver Ansatz, um Computersysteme, Netzwerke und andere Geräte vor Cyberattacken effektiv zu schützen. Das Ziel ist es, die Auswirkungen eines solchen Angriffs so gut es geht zu minimieren und das wertvollste Gut Ihres Unternehmens, die Daten, zu schützen.

Service Process

Nach der Festlegung des Umfangs und der Unterzeichnung einer Vertraulichkeitsvereinbarung führen wir die folgenden Prozesse durch:

- **Regeln und Vereinbarung zur Zusammenarbeit**
- **Planung**
- **Ausführung**
- **Post-Ausführung**
- **Bewertung nach der Behebung der Schwachstell**

Nach der Analyse erhalten Sie einen Bericht, in dem wir die festgestellten Schwachstellen und mögliche Abhilfemaßnahmen untersuchen. Die Methodik, die wir bei allen unseren Dienstleistungen anwenden, basiert auf Industriestandards.

EYESIGHT - Public Discovery Scan (kostenlos)

EYESIGHT ist ein kostenloser OSINT Service, mit dem wir Organisationen dabei helfen, das Risikoniveau zu ermitteln, welchem sie ausgesetzt sind. Dies basiert auf der Grundlage der öffentlichen Informationen, welche im Internet über das Unternehmen verfügbar sind.

Einzig und allein der Domainname reicht aus, um eine OSINT Analyse zu einer zugehörigen Domain durchzuführen und herauszufinden, welche Daten für jedermann sichtbar und frei zugänglich im Internet verfügbar sind. und werden von den Robotern der Cyberangreifer kontinuierlich verfolgt und bilden die Grundlage für jeden massiven oder gezielten Angriff.

External Penetration Testing

Ziel ist es, einen Angriff von außerhalb der IT-Infrastruktur zu simulieren. Es werden alle, dem Internet ausgesetzten Assets, die ein Angreifer als Einstiegspunkt in sein Unternehmensnetzwerk verwenden kann, identifiziert und bewertet.

Wir verwenden automatisierte Tools und manuelle Vorgehensweisen, um die Wirksamkeit Ihrer Sicherheitsmechanismen wie Firewalls und Intrusion-Prevention-Systeme zu evaluieren.

Offensive Security Services

Internal Penetration Testing

Simuliert einen Angriff, der innerhalb des Sicherheitsperimeters einer Organisation ausgeführt wird.

Ziel ist es, die Auswirkungen eines internen Angriffs, beispielsweise eines bösartigen Mitarbeiters, zu bewerten. Der Prozess ist immer auf die Bedürfnisse des Kunden zugeschnitten, es sollte jedoch beachtet werden, dass es in der Regel um die Identifizierung von gefährdeten Instanzen und der Exfiltration geschäftskritischer Informationen geht.

Evaluation of Active Directory

Active Directory (AD) Penetrationstests in einer Windows-Umgebung bestehen darin, die Aktionen eines Angreifers zu simulieren, der Zugang zum Unternehmensnetz hat. Dieser Zugang könnte physisch oder über eine infizierte Workstation erfolgen.

Das Hauptziel besteht darin, Schwachstellen zu finden, die sich auf die Grenzen des Unternehmens auswirken, und Aktionspläne zur Verbesserung der Sicherheitslage des AD vorzuschlagen.

Das Ziel der Active-Directory-Prüfung besteht darin, Sicherheitsprobleme innerhalb des internen Netzwerks einer Organisation zu identifizieren.

Web Application Penetration Test

Ziel von Penetrationstests für Webanwendungen ist es, die Sicherheitslage von Webanwendungen zu bewerten, indem Schwachstellen, die aus unsicheren Design- und Implementierungspraktiken resultieren, identifiziert und untersucht werden.

Sie erfolgt durch den Einsatz automatisierter und manueller Tools zur Validierung der Wirksamkeit von Sicherheitsmechanismen, wie z. B. der Web Application Firewall WAF.

API Penetration Test

Penetrationstests für Application Programming Interfaces (APIs) konzentrieren sich auf die Bewertung der Sicherheitslage von Umgebungen, die APIs verwenden und eine Datenübertragung erfordern.

Ziel ist es, die Logik der Anwendung zu modifizieren und festzustellen, ob über eingeschränkte Funktionalitäten und Zugriffsebenen eine Preisgabe möglicherweise sensibler Informationen zu erreichen ist. Bei den Tests werden hauptsächlich Enumeration- und Exploitation-Techniken eingesetzt, die im OWASP API Testing Guide beschrieben sind.

Vulnerability Assessment

Ziel des Vulnerability Assessments ist es, Schwachstellen in Netzwerken, Datenbanken und Anwendungen zu identifizieren, zu klassifizieren und nach Prioritäten zu ordnen.

Das Engagement ist umfassender und komplizierter als bei gewöhnlichen Scans, da es auch benutzerdefinierte Testrichtlinien umfasst, um Verstöße und Fehlkonfigurationen von Instanzen im Netzwerk des Kunden zu erkennen. Anhand der gesammelten Informationen werden die Schwachstellen klassifiziert und auf der Grundlage der branchenüblichen Best Practices für das Risikomanagement nach Prioritäten geordnet. Hinsichtlich der Arten von Schwachstellenbewertungen können die Verpflichtungen Folgendes umfassen:

- **Netzwerk- und Wireless-Assessments**
- **Host-Evaluierungen**
- **Datenbank-Evaluierungen**
- **Analyse von Anwendungen**

Mobile Application Penetration Test

Das Ziel von Penetrationstests für mobile Anwendungen ist es, Sicherheitslücken in benutzerdefinierten mobilen Anwendungen auf Android- und iOS-Plattformen zu identifizieren.

Wir bewerten die Sicherheit einer Anwendung sowohl durch statische als auch durch dynamische Analyse gemäß den Testrichtlinien des Open Web Application Security Project (OWASP).

Cloud Environment Penetration Test

Cloud-Penetrationstests konzentrieren sich auf Design-, Bereitstellungs- und Konfigurationsfehler in Cloud-gehosteten Umgebungen. Unsere Cybersicherheits-Experten verwenden eine breite Palette von Tools, Techniken und Verfahren, um die Sicherheitslage eines Unternehmens sowohl aus externer als auch aus interner Sicht zu bewerten.

Fehlkonfigurationen und mangelhafte Zugangsrichtlinien sind der Hauptgrund für Security Breaches. Wir helfen unseren Kunden, die Risiken zu verstehen und schlagen Maßnahmen vor, um ein sichereres IT-Ökosystem zu schaffen.

Wi-Fi Penetration Testing

Ziel des Wi-Fi-Penetrationstests ist es, Sicherheitslücken in den aktuellen Wi-Fi-Netzwerken zu identifizieren.

Wi-Fi-Penetrationstests können auch den Einsatz von Social Engineering beinhalten. Die Nutzer zur Preisgabe ihres Wi-Fi-Passworts zu verleiten, oder ihren Datenverkehr zu manipulieren, sind gängige Angriffsvektoren.

VoIP Penetration Testing

Voice over Internet Telephony Protocol (VoIP) ist eine Technologie, die fortschrittliche und effiziente Kommunikationslösungen bietet. VoIP bietet viele zusätzliche Funktionen und folglich auch weitere Angriffsmöglichkeiten. Um die Sicherheitslage eines Unternehmens zu stärken, ist eine Eindämmung dieser Gefahrenvektoren unerlässlich.

Ziel des VoIP-Penetrationstests ist es, Sicherheitslücken in der/den aktuellen VoIP-Infrastruktur-Implementierung(en) zu identifizieren.

Phishing Campaign Services

Phishing ist eine enorme Bedrohung, die sich von Jahr zu Jahr stärker ausbreitet und als zweitteuerste Ursache für Datenschutzverletzungen gilt.

Ingram Micro bietet maßgeschneiderte Phishing-Kampagnen, die von unseren Service-Spezialisten für jede Art von Unternehmen durchgeführt werden, unabhängig von der Größe, dem Sektor oder den spezifischen Anforderungen.

Cyber Security Assessment Tool (CSAT)

Erstellen Sie Ihren risikobasierten Cybersicherheitscheck basierend auf einer automatisierten Datenerhebung und Schwachstellenanalyse des Netzwerks. Ihr Begleiter für Sicherheit und Compliance (GDPR).

Das Cyber Security Assessment Tool (CSAT) verschafft den IT-Teams eines Unternehmens schnell einen Einblick in potenzielle Cyber-Risiken und hilft ihnen zu entscheiden, wo und wie sie ihre Sicherheitsmaßnahmen verbessern können.

CSAT scannt auf schnellem Wege die gesamte Unternehmensinfrastruktur, einschließlich Microsoft 365 und Azure-Abonnements, auf potenzielle Schwachstellen und Risikobereiche, um intelligente und gerechtfertigte Investitionen in die Sicherheit zu ermöglichen, die sich auf die Schwachstellen des Unternehmens konzentrieren

Cyber Threat Intelligence (OSINT)

Bei einer Cyber-Bedrohungsanalyse betrachten unsere zertifizierten Ethical Hacker ihr Unternehmen als ihr Ziel und sammeln die Informationen, die sie für einen effektiven Angriff benötigen würden.

Die Informationen, nach denen wir bei einer Bedrohungsanalyse suchen, könnten Angreifern dabei helfen, sich bspw. Für eine Phishingmail als hochrangige Entscheidungsträger auszugeben, effektivere Cyberangriffe zu starten, Social-Engineering-Kampagnen zu initiieren und anschließend Ihre Sicherheit zu gefährden. Diese Informationen werden verwendet, um auf Cyber-Bedrohungen, die jene öffentlich zugänglichen Informationen für einen Angriff verwenden würden, zu verhindern und zu identifizieren.

IoT Penetration Testing

Im modernen Internet machen Internet-of-Things-Geräte (IoT) einen wachsenden Anteil der mit dem Internet verbundenen Geräte aus, und mit dem Aufkommen von 5G wird das IoT voraussichtlich noch größer werden.

Im Rahmen des IoT-Penetrationstests identifizieren wir die Sicherheitslücken, die durch die Nutzung von IoT-Geräten entstehen und den Kunden für Angreifer anfällig machen können. Dabei analysieren und testen wir das gesamte Ökosystem der IoT-Geräte (von der Hardware bis zur Cloud) und bewerten die Sicherheitslage des Kunden in Bezug auf IoT. Das endgültige Ziel besteht darin, die Schwachstellen genau zu identifizieren und eine Gesamtrisikobewertung zu berechnen, die dem Kunden eine globale und klare Vorstellung von den Angriffswegen und den möglichen Auswirkungen vermittelt und detaillierte und maßgeschneiderte Abhilfemaßnahmen vorschlägt, um alle Probleme zu beheben oder abzuschwächen und den Kunden so gut wie möglich zu schützen.

INGRAM MICRO
SECURITY