INGRAM MICRO SECURITY

Cyber Security Services

Dienstleistungskatalog

Offensive Security Services

Dienstleistungen im Bereich der Cybersicherheit von Ingram Micro

CENTER OF EXCELLENCE CYBER SECURITY

INHALT

ANSPRECHPARTNER

Christian Voss-Freund
System Engineer
Tel. +49.89.4208.2629
christian.voss-freund@ingrammicro.com

Cyber Security Business Unit
cybersecurity@ingrammicro.de

EINFÜHRUNG

Offensive Sicherheit bedeutet, dass aktiv die Rolle des Angreifers eingenommen wird und dadurch Einfallstore in Computersysteme, Netzwerke und Einzelpersonen proaktiv erkannt werden. Konventionelle Sicherheitsmaßnahmen – manchmal „defensive Sicherheit“ genannt – sind vor allem reaktiv. Zu diesen Maßnahmen zählen unter anderem Sicherheitslösungen oder auch das Suchen und Beheben von Schwachstellen im System. Im Gegensatz dazu geht es bei der offensiven Sicherheit um die Simulation echter Angriffe von außen.

Wir möchten Unternehmen dabei helfen, sich bestmöglich vor Cyberangriffen zu schützen. Das „Ingram Micro Cyber Security Center of Excellence“-Team wurde mit dem Ziel gegründet, unser Unternehmen dabei zu unterstützen, das Potenzial der Cybersicherheit auszuschöpfen. Das europäische Team mit Sitz in den Niederlanden bietet eine Auswahl spezieller Beratungs- und Schulungslösungen zum Thema Cybersicherheit für unsere Business- und Channel-Partner.

Unser Beratungsteam im Bereich Cybersicherheit bündelt umfassende Expertise zu offensiven Sicherheitsmaßnahmen und Erfahrung in verschiedensten Sektoren weltweit.

Gerne stehen wir Ihnen für weitere Informationen zur Verfügung: cs-coe-weur@ingrammicro.com

UNSER DIENSTLEISTUNGSPROZESS

Alle Dienstleistungen werden auf der Grundlage einer Leistungsbeschreibung erbracht. Demnach erfolgt die Preissetzung anhand der berechneten Beratungstagessätze pro Dienstleistung.

PLANUNG

Die Planungsphase ist entscheidend für den Erfolg des Auftrags. In dieser Phase werden die für die Analyse erforderlichen Informationen zusammengetragen. Dazu zählen Informationen zu u. a. den zu testenden IT-Komponenten, den relevanten Bedrohungen für diese Komponenten, etwaigen relevanten Dokumentationen sowie den im Analyseansatz zur Risikominderung anzuwendenden Sicherheitskontrollen.

Eine Sicherheitsanalyse erfolgt wie für jedes andere Projekt auf der Grundlage eines Projektmanagementplans, in dem die Ziele und Ergebnisse, der Leistungsumfang, die Anforderungen, die Rollen und Zuständigkeiten sowie die Grenzen, Erfolgsfaktoren, Annahmen, Ressourcen, zeitliche Planung und Liefergegenstände niedergelegt sind.

AUFTRAGSBEDINGUNGEN

Nach dem Projektstart werden die Anforderungen des Kunden ermittelt, auf deren Grundlage Ingram Micro einen Entwurf für die Leistungsbeschreibung („Statement of Work“) aufsetzt. Nach Einigung über die Bestimmungen der Leistungsbeschreibung wird der Leistungsumfang umfassend spezifiziert. Dies beinhaltet das Aufsetzen und die Unterzeichnung des Testgenehmigungsschreibens durch beide Parteien sowie eine kurze Besprechung zur Endabstimmung der zeitlichen Planung und Kommunikationsdetails.
Das Testgenehmigungsschreiben dient der Bestätigung der Auftragsbedingungen und der Beantwortung aller Fragen vor dem Projektbeginn.

AUSFÜHRUNG

Unsere Dienstleistungen im Bereich der offensiven Sicherheit werden von einem Team aus zertifizierten, sehr erfahrenen Expertinnen bzw. Experten ausgeführt. Sie wenden branchenübliche bewährte Verfahren sowie Tools und Techniken an, wie sie auch bei echten Angriffen verwendet werden.
Neben gewerblichen Produkten kommen auch unternehmenseigene Software und Skripte zum Einsatz, mittels derer sich Angriffe noch besser simulieren lassen.

NACH DER AUSFÜHRUNG

Nach dem Abschluss der Ausführungsphase dokumentiert Ingram Micro alle Erkenntnisse in einem Bericht. Dieser Bericht wird zunächst der internen Qualitätssicherung unterzogen, bevor der Abschlussbericht innerhalb von zwei Wochen nach Auftragsabschluss an den Kunden übermittelt wird.

Dieser Bericht rundet den Auftrag ab und besteht aus einer allgemeinen Zusammenfassung, die als Grundlage für strategische Unternehmensentscheidungen dienen kann, sowie auf einer ausführlichen Analysebeschreibung, anhand derer sich die technischen Aspekte der Tests nachvollziehen lassen.

Der Bericht gliedert sich in die folgenden Abschnitte:

- Allgemeine Zusammenfassung
- Technische Zusammenfassung
- Analysebeschreibung
- Erkenntnisse
- Anhänge (mit Scanergebnissen und Erläuterungen zur Methodik)

ÜBERPRÜFUNG DER ERGRIFFENEN KORREKTURMASSNAHMEN

Falls das Unternehmen die Korrekturmaßnahmen, die zur Behebung der ermittelten Schwachstellen unternommen wurden, überprüfen möchte, führt Ingram Micro diese Überprüfung gerne gegen Aufpreis durch. Eine solche Überprüfung wird dringend empfohlen. Für weitere Informationen und die zeitliche Planung steht Ihnen Ihr Channel-Partner gerne zur Verfügung.

DIENSTLEISTUNGSPORTFOLIO

Ingram Micro EYESIGHT – Public-Discovery-Scan

EINFÜHRUNG

Vorfälle im Bereich der Cybersicherheit nehmen zu und Unternehmen jeder Größe weltweit und in jedem Industriesektor sind Ziel von Hackerangriffen. Bevor sie ein Ziel auswählen, suchen Hacker üblicherweise nach im Internet verfügbaren und allen Nutzern zugänglichen Informationen über das Unternehmen.
Dies bietet überraschenderweise oftmals sehr nützliche Informationen, die Hacker zu einem späteren Zeitpunkt verwenden können, um sich Zugang zu den Systemen und Informationen des ausgewählten Unternehmens zu verschaffen und diese zu manipulieren.

Ingram Micro EYESIGHT ist ein von Ingram Micro angebotener kostenloser Service, mit dem Unternehmen ermitteln können, welchem Risiko sie durch eine unzureichende Kontrolle über die im Internet veröffentlichten Informationen ausgesetzt sind.

ZWECK DER DIENSTLEISTUNG

Im Rahmen des EYESIGHT-Tests von Ingram Micro werden öffentlich verfügbare personenbezogene und/oder sensible Daten über das betreffende Unternehmen gesammelt. Diese Informationen sind in der Regel allgemein im Internet verfügbar. Im Anschluss werden solche Informationen vor dem Hintergrund eines möglichen Datendiebstahls geprüft. Diese Prüfung legt schnell und einfach mögliche grundlegende Sicherheitsrisiken von außen offen.

LEISTUNGSUMFANG

Mit dem EYESIGHT-Test von Ingram Micro wird nach allen öffentlich verfügbaren Unternehmensinformationen gesucht. Dies beinhaltet unter anderem IP-Adressen, Webadressen, E-Mail-Adressen, Word-Dateien, PowerPoint-Präsentationen, PDF-Dokumente und andere Informationen, die für Hacker interessant sein könnten.

PROZESS DES EYESIGHT-TESTS VON INGRAM MICRO

Im Rahmen des EYESIGHT-Tests von Ingram Micro werden Daten passiv und ohne Eindringen gesammelt. Es werden keine aktiven Scans durchgeführt und der Prozess umfasst nur minimale Interaktionen mit den Systemen des Unternehmens. Der Test wird üblicherweise ausschließlich mit dem Domainnamen des Unternehmens durchgeführt.
Alle im Rahmen des Tests genutzten Informationen werden durch Google-Suchen und andere Tools der Informationsgewinnung aus öffentlich verfügbaren Quellen (Open-Source-Intelligence, OSINT) erhoben.

VORAUSSETZUNGEN

Name und Domäne des betreffenden Unternehmens.

LIEFERGEGENSTÄNDE

Nach Abschluss des EYESIGHT-Tests von Ingram Micro erhält der Kunde einen ausführlichen Bericht, der Folgendes enthält:

- **Allgemeine Zusammenfassung:**
  Eine Zusammenfassung des Zwecks der Analyse sowie eine kurze Erläuterung der geschäftlichen Bedrohungen, denen das Unternehmen ausgesetzt ist.
- **Erkenntnisse:**
  Eine ausführliche technische Erläuterung der Erkenntnisse der Analyse zusammen mit Schritten und Nachweisen der Erkenntnisse.
- **Schlussfolgerung und Empfehlungen:**
  Dieser Abschnitt enthält abschließende Empfehlungen und eine Zusammenfassung der während der Sicherheitsanalyse festgestellten Probleme.

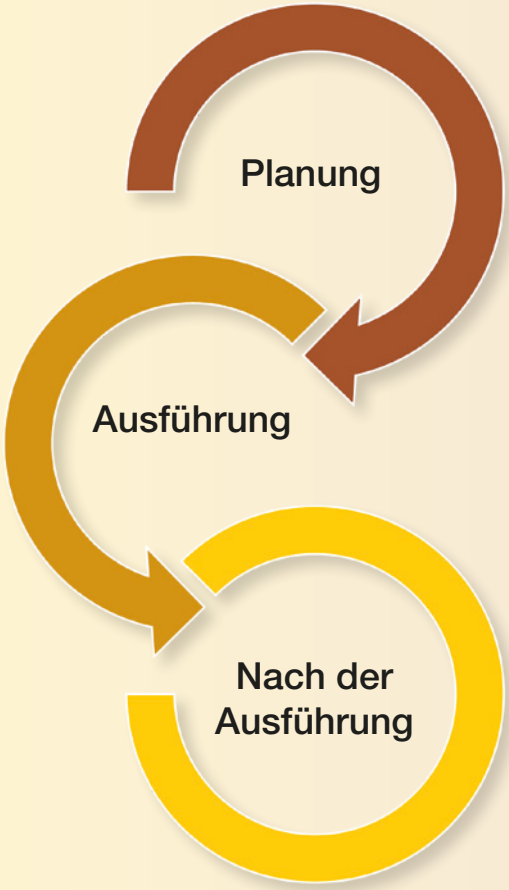
Externer Penetrationstest

Zweck des externen Penetrationstests ist die Simulation eines Angriffs aus dem öffentlichen Internet. Im Rahmen dieses Auftrags sollen alle vom Internet aus zugänglichen IT-Komponenten, über die Angriffe auf das Netzwerk Ihres Unternehmens ausgeübt werden könnten, identifiziert und analysiert werden.

Dabei wird mittels automatisierter und manueller Tools die Wirksamkeit Ihrer Schutzmechanismen, z. B. Ihrer Firewalls und Intrusion-Prevention-Systeme, überprüft.

Unsere Methodik gründet u. a. auf den folgenden Branchenstandards:

- NIST 800-115
- Penetration Testing Execution Standard (PTES)
- Open Web Application Security Project (OWASP) Testing Guide
- Payment Card Industry (PCI) Penetration Testing Guidance
- Open-Source Security Testing Methodology Manual (OSSTMM)



- Sammeln von Informationen zwecks Festlegung des Leistungsumfangs
- Bestätigung der Leistungsbeschreibung
- Aufsetzen des Testgenehmigungsschreibens

- Reconnaissance
- Bedrohungsmodellierung
- Schwachstellenanalyse
- Exploitation
- Post-Exploitation

- Erstellung des Berichts
- Qualitätssicherung
- Präsentation

LEISTUNGSUMFANG

Der externe Penetrationstest ist ausdrücklich auf von außen zugängliche Geräte des betreffenden Unternehmens beschränkt. Er bezieht sich im Wesentlichen auf die OSI-Schichten 4 (Transportschicht) und 6 (Darstellungsschicht), umfasst aber auch Open-Source-Intelligence-Tätigkeiten (OSINT).

Ziel ist es, sensible Daten zu identifizieren – etwa zugänglich gewordene Zugriffsschlüssel für Cloud Umgebungen, durch Datenschutzverletzungen zugänglich gewordene Daten, Informationen aus öffentlichen Datenbeständen usw. –, die für Angriffe genutzt werden könnten. Auf Servern gehostete Anwendungen werden nur am Rande geprüft. Deren Prüfung erfolgt im Rahmen des Webanwendungstests.

GRENZEN DES LEISTUNGSUMFANGS

Das Folgende ist **NICHT Bestandteil** dieses Angebots:

- Implementierung von Maßnahmen und Empfehlungen zur Risikominderung
- Sicherheitshärtung, Behebung von Schwachstellen, Patching und Entwicklung von Modulen zur Risikominderung
- Denial-of-Service-Test und -Exploit
- sämtliche Tätigkeiten, die nicht ausdrücklich in dieser Dienstleistungsbeschreibung niedergelegt sind

PLANUNG

Die Planungsphase ist entscheidend für den Erfolg des Auftrags. In dieser Phase werden die für die Analyse erforderlichen Informationen zusammengetragen. Dazu zählen Informationen zu u. a. den zu testenden IT-Komponenten, den relevanten Bedrohungen für diese Komponenten sowie den im Analyseansatz zur Risikominderung anzuwendenden Sicherheitskontrollen.
Eine Sicherheitsanalyse erfolgt wie jedes andere Projekt auf der Grundlage eines Projektmanagementplans, in dem die Ziele und Ergebnisse, der Leistungsumfang, die Anforderungen, die Rollen und Zuständigkeiten sowie die Grenzen, Erfolgsfaktoren, Annahmen, Ressourcen, zeitliche Planung und Liefergegenstände niedergelegt sind.

Nach dem Projektstart werden die Anforderungen des Kunden erhoben, auf deren Grundlage Ingram Micro einen Entwurf für die Leistungsbeschreibung aufsetzt. Nach Einigung über die Bestimmungen der Leistungsbeschreibung wird der Leistungsumfang umfassend spezifiziert. Dies beinhaltet das Aufsetzen und die Unterzeichnung des Testgenehmigungsschreibens durch beide Parteien sowie eine kurze Besprechung zur Endabstimmung der zeitlichen Planung und Kommunikationsdetails. Das Testgenehmigungsschreiben dient der Bestätigung der Auftragsbedingungen und der Beantwortung aller Fragen vor dem Projektbeginn.

PENETRATIONSTEST FÜR NETZWERKE – METHODIK

Die Penetrationstests von Ingram Micro verzichten auf detaillierte Netzwerk- oder Infrastrukturdiagramme sowie auf Konten oder zusätzliche Benutzerinformationen, es sei denn, dies ist laut Leistungsumfang vorgesehen.

Unsere Methodik für externe Penetrationstests umfasst das Folgende:

Reconnaissance

- Informationsgewinnung anhand öffentlich verfügbarer Informationen
- Footprinting
- DNS-Analyse und DNS-Bruteforcing

Bedrohungsmodellierung

- Port-Scan
- System-Fingerprinting
- Enumeration

Schwachstellenanalyse

- Vorbereitung der Exploitation

Exploitation

- Manuelle Schwachstellenprüfung und Verifizierung identifizierter Schwachstellen
- Prüfung von Firewalls und Intrusion-Detection- bzw. -Prevention-Systemen
- Passwort-Spraying mit gängigen und schwachen Passwörtern

Post-Exploitation

- Enumeration im lokalen System
- Enumeration im Netzwerk und Pivoting
- Identifizierung sensibler Daten
- Exfiltration

Der externe Netzwerktest kann auf einen ausgewählten IP-Bereich beschränkt werden oder die erweiterte Reconnaissance mittels OSINT (Open-Source-Intelligence) umfassen.

TOOLS

Ingram Micro verwendet sowohl branchenübliche Tools und Frameworks als auch unsere eigenen Skripte. Auf diese Weise gewährleisten wir, dass unsere Penetrationstests möglichst lückenlos und umfassend sind.

Bei unseren Penetrationstests setzen wir u. a. die folgenden Tools ein:

- Amass
- theHarvester/Pyfoca
- Recon-ng
- Maltego
- Nmap
- Nessus Professional
- Testssl.sh
- Ike-Scan
- Aquatone/Eyewitness
- Burp Suite Pro
- Dirbuster/Dirb/GoBuster
- Nikto
- Sqlmap
- Metasploit Framework
- Custom Scripts

NACH DER AUSFÜHRUNG

Nach dem Abschluss der Ausführungsphase dokumentiert Ingram Micro alle Erkenntnisse in einem Bericht. Dieser Bericht wird zunächst der internen Qualitätssicherung unterzogen, bevor der Abschlussbericht innerhalb von zwei Wochen nach Auftragsabschluss an den Kunden übermittelt wird.

Dieser Bericht rundet den Auftrag ab und besteht aus einer allgemeinen Zusammenfassung, die als Grundlage für strategische Unternehmensentscheidungen dienen kann, sowie auf einer ausführlichen Analysebeschreibung, anhand derer sich die technischen Aspekte der Tests nachvollziehen lassen.

Der Bericht gliedert sich in die folgenden Abschnitte:

- Allgemeine Zusammenfassung
- Technische Zusammenfassung
- Analysebeschreibung
- Erkenntnisse
- Anhänge (mit Scanergebnissen und Erläuterungen zur Methodik)

ÜBERPRÜFUNG DER ERGRIFFENEN KORREKTURMASSNAHMEN

Falls das Unternehmen die Korrekturmaßnahmen, die zur Behebung der ermittelten Schwachstellen unternommen wurden, überprüfen möchte, führt Ingram Micro diese Überprüfung gerne gegen Aufpreis durch. Für weitere Informationen und die zeitliche Planung steht Ihnen Ihr Channel-Partner gerne zur Verfügung.

PFLICHTEN DES KUNDEN

Der Kunde verpflichtet sich zur Erfüllung seiner Pflichten und erkennt an und erklärt sich damit einverstanden, dass **die Erfüllung der Pflichten von Ingram Micro von dem Folgenden abhängt:**

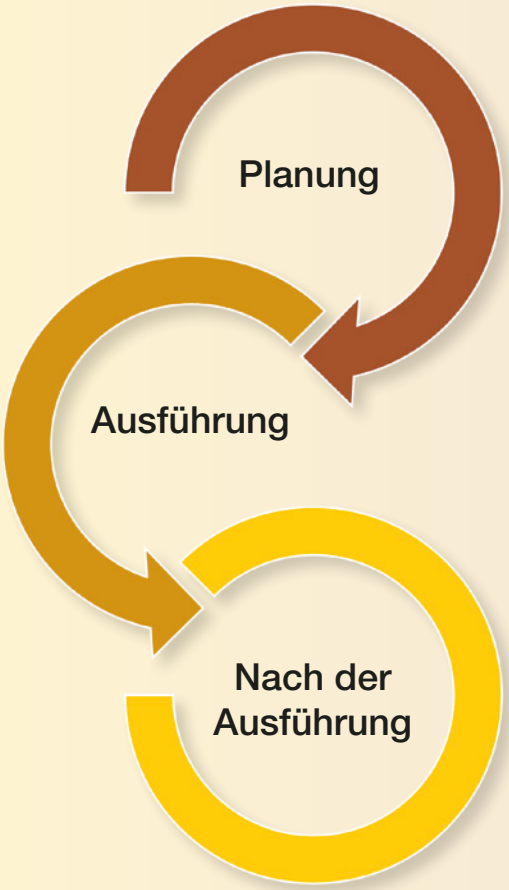
- Die Ressourcen des Kunden stehen Ingram Micro plangemäß zur Verfügung.
- Alle zu analysierenden Server und Netzwerke sind bei Durchführung der Analyse in Betrieb und funktionsfähig.
- Der Kunde stellt sämtliche angefragten Dokumente und Informationen rechtzeitig und im Einklang mit den in der Planungsphase festgelegten Lieferterminen zur Verfügung.
- Zu Testzwecken wird jede im Leistungsumfang enthaltene IP als separater Host betrachtet, und zwar unabhängig vom potenziellen Lastenausgleich, von Firewalls usw.
- Sofern keine anderweitigen Bedingungen mit dem Unternehmen vereinbart wurden, werden sämtliche Test- und Analysetätigkeiten in einem Zeitfenster von 24 Stunden durchgeführt.
- Die Testzeitfenster des Kunden müssen lange genug für die Durchführung der Tätigkeiten sein.

Interner Penetrationstest

Der interne Penetrationstest simuliert einen Angriff, der von innerhalb der Sicherheitszone des Unternehmens aus durchgeführt wird. Dabei werden die Auswirkungen eines Angriffs durch einen Insider, etwa einen verärgerten Mitarbeiter, analysiert. Der Prozess ist stets auf die Anforderungen des Kunden abgestimmt, umfasst jedoch in der Regel die Identifizierung von Schwachstellen bei Instanzen sowie die Exfiltration von geschäftskritischen Daten.

Unsere Methodik gründet u. a. auf den folgenden Branchenstandards:

- NIST 800-115
- Penetration Testing Execution Standard (PTES)
- MITRE ATT&CK
- Payment Card Industry (PCI) Penetration Testing Guidance
- Open-Source Security Testing Methodology Manual (OSSTMM)



- Sammeln von Informationen zwecks Festlegung des Leistungsumfangs
- Bestätigung der Leistungsbeschreibung
- Aufsetzen des Testgenehmigungsschreibens

- Reconnaissance
- Bedrohungsmodellierung
- Schwachstellenanalyse
- Exploitation
- Post-Exploitation

- Erstellung des Berichts
- Qualitätssicherung
- Präsentation

LEISTUNGSUMFANG

Der interne Penetrationstest zielt auf den Angriff der verbundenen Instanzen im Netzwerk des betreffenden Unternehmens. Er bezieht sich im Wesentlichen auf die OSI-Schichten 3 (Netzwerkschicht) bis 7 (Anwendungsschicht), umfasst aber auch Angriffe auf Schicht 2 (Sicherungsschicht), sofern das Testteam von Ingram Micro direkten Zugang zu einem Gerät vor Ort hat.

Auf Wunsch des Kunden kann Ingram Micro einen Segmentationstest gemäß PCI DSS durchführen. Zudem können Analysen auf der Grundlage eines „Assumed Compromise"-Szenarios durchgeführt werden. Diese dienen der Überprüfung von Active-Directory-Konfigurationen, indem sie eine bereits erfolgte unbefugte Eskalation der Zugangsrechte oder Lateral-Movement-Angriffe innerhalb der Unternehmensumgebung simulieren.

Zweck des internen Penetrationstests ist es, sensible Daten zu identifizieren, die sich als Ziel von Angriffen anbieten.

GRENZEN DES LEISTUNGSUMFANGS

Das Folgende ist **NICHT Bestandteil** dieses Angebots:

- Implementierung von Maßnahmen und Empfehlungen zur Risikominderung
- Sicherheitshärtung, Behebung von Schwachstellen, Patching und Entwicklung von Modulen zur Risikominderung
- Denial-of-Service-Test und -Exploit
- Sofern nicht anderweitig gewünscht, wird der Penetrationstest möglichst transparent durchgeführt.
- sämtliche Tätigkeiten, die nicht ausdrücklich in dieser Dienstleistungsbeschreibung niedergelegt sind

UNSER DIENSTLEISTUNGSPROZESS

Planung

- Sammeln von Informationen zwecks Festlegung des Leistungsumfangs
- Bestätigung der Leistungsbeschreibung
- Aufsetzen des Testgenehmigungsschreibens

Ausführung

- Reconnaissance
- Bedrohungsmodellierung
- Schwachstellenanalyse
- Exploitation
- Post-Exploitation

Nach der Ausführung

- Erstellung des Berichts
- Qualitätssicherung
- Präsentation

PLANUNG

Die Planungsphase ist entscheidend für den Erfolg des Auftrags. In dieser Phase werden die für die Analyse erforderlichen Informationen zusammengetragen. Dazu zählen Informationen zu u. a. den zu testenden IT-Komponenten, den relevanten Bedrohungen für diese Komponenten sowie den im Analyseansatz zur Risikominderung anzuwendenden Sicherheitskontrollen. Eine Sicherheitsanalyse erfolgt wie jedes andere Projekt auf der Grundlage eines Projektmanagementplans, in dem die Ziele und Ergebnisse, der Leistungsumfang, die Anforderungen, die Rollen und Zuständigkeiten sowie die Grenzen, Erfolgsfaktoren, Annahmen, Ressourcen, zeitliche Planung und Liefergegenstände niedergelegt sind.

Nach dem Projektstart werden die Anforderungen des Kunden erhoben, auf deren Grundlage Ingram Micro einen Entwurf für die Leistungsbeschreibung aufsetzt. Nach Einigung über die Bestimmungen der Leistungsbeschreibung wird der Leistungsumfang umfassend spezifiziert. Dies beinhaltet das Aufsetzen und die Unterzeichnung des Testgenehmigungsschreibens durch beide Parteien sowie eine kurze Besprechung zur Endabstimmung der zeitlichen Planung und Kommunikationsdetails. Das Testgenehmigungsschreiben dient der Bestätigung der Auftragsbedingungen und der Beantwortung aller Fragen vor dem Projektbeginn.

PENETRATIONSTEST FÜR NETZWERKE – METHODIK

Ingram Micro führt den Penetrationstest über einen Remote-VPN-Zugang zum betreffenden Netzwerksegment, über ein Gerät vor Ort oder eine vom Kunden betriebene Instanz durch.

Unsere Methodik für interne Penetrationstests umfasst das Folgende:

Reconnaissance

- Sniffing und passive Informationsgewinnung
- Traffic-Analyse

Discovery

- Port-Scan
- System-Fingerprinting
- Netzwerk-Scan/Host-Discovery
- Enumeration

Schwachstellenanalyse

- Vorbereitung der Exploitation

Exploitation

- Manuelle Schwachstellenprüfung und Verifizierung identifizierter Schwachstellen
- Prüfung von Firewalls und Intrusion-Detection- bzw. -Prevention-Systemen
- Passwort-Spraying mit gängigen und schwachen Passwörtern

Post-Exploitation

- Enumeration im lokalen System
- Enumeration im Netzwerk und Pivoting
- Identifizierung sensibler Daten
- Exfiltration

TOOLS

Ingram Micro verwendet sowohl branchenübliche Tools und Frameworks als auch unsere eigenen Skripte. Auf diese Weise gewährleisten wir, dass unsere Penetrationstests möglichst lückenlos und umfassend ist.

Bei unseren Penetrationstests setzen wir u. a. die folgenden Tools ein:

- Wireshark/tcpdump
- CrossLinked
- theHarvester/Pyfoca
- Respoder
- Mitm6
- Nmap
- Nessus Professional
- CrackMapExec
- Impacket
- Aquatone/Eyewitness
- Burp Suite Pro
- Dirbuster/Dirb/GoBuster
- Hashcat
- Metasploit Framework
- Command & Control Frameworks
- Custom Scripts

NACH DER AUSFÜHRUNG

Nach dem Abschluss der Ausführungsphase dokumentiert Ingram Micro alle Erkenntnisse in einem Bericht. Dieser Bericht wird zunächst der internen Qualitätssicherung unterzogen, bevor der Abschlussbericht innerhalb von zwei Wochen nach Auftragsabschluss an den Kunden übermittelt wird.
Dieser Bericht rundet den Auftrag ab und besteht aus einer allgemeinen Zusammenfassung, die als Grundlage für strategische Unternehmensentscheidungen dienen kann, sowie auf einer ausführlichen Analysebeschreibung, anhand derer sich die technischen Aspekte der Tests nachvollziehen lassen.

Der Bericht gliedert sich in die folgenden Abschnitte:

- Allgemeine Zusammenfassung
- Technische Zusammenfassung
- Analysebeschreibung
- Erkenntnisse
- Anhänge (mit Scanergebnissen und Erläuterungen zur Methodik)

ÜBERPRÜFUNG DER ERGRIFFENEN KORREKTURMASSNAHMEN

Falls das Unternehmen die Korrekturmaßnahmen, die zur Behebung der ermittelten Schwachstellen unternommen wurden, überprüfen möchte, führt Ingram Micro diese Überprüfung gerne gegen Aufpreis durch.
Für weitere Informationen und die zeitliche Planung steht Ihnen Ihr Channel-Partner gerne zur Verfügung.

PFLICHTEN DES KUNDEN

Der Kunde verpflichtet sich zur Erfüllung seiner Pflichten und erkennt an und erklärt sich damit einverstanden, dass **die Erfüllung der Pflichten von Ingram Micro von dem Folgenden abhängt:**

- Die Ressourcen des Kunden stehen Ingram Micro plangemäß zur Verfügung.
- Alle zu analysierenden Server und Netzwerke sind bei Durchführung der Analyse in Betrieb und funktionsfähig.
- Der Kunde stellt sämtliche angefragten Dokumente und Informationen rechtzeitig und im Einklang mit den in der Planungsphase festgelegten Lieferterminen zur Verfügung.
- Zu Testzwecken wird jede im Leistungsumfang enthaltene IP als separater Host betrachtet, und zwar unabhängig vom potenziellen Lastenausgleich, von Firewalls usw.
- Sofern keine anderweitigen Bedingungen mit dem Unternehmen vereinbart wurden, werden sämtliche Test- und Analysetätigkeiten in einem Zeitfenster von 24 Stunden durchgeführt.
- Die Testzeitfenster des Kunden müssen lange genug für die Durchführung der Tätigkeiten sein.

Es gelten die vor Ort anwendbaren Allgemeine Geschäftsbedingungen von Ingram Micro.

Penetrationstest für Active Directory

Active Directory ist ein Verzeichnisdienst, der von Microsoft für das Windows-Domänennetzwerk entwickelt wurde. Innerhalb von IT-Infrastrukturen von Unternehmen wird der Dienst meist zur Verwaltung von Benutzern und Computern mit einem einzigen Kontrollpunkt, dem „Domänen-Controller“, verwendet. Über 90 % der umsatzstärksten Unternehmen der Welt setzen beim wirksamen Management ihrer Ressourcen auf Active Directory.

Bei einem Penetrationstest für Active Directory in einer Windows-Umgebung wird ein Angriff per Zugang zum Unternehmensnetzwerk simuliert. Dieser Zugang kann physisch oder über einen infizierten Arbeitsplatzrechner erfolgen. Vorrangig geht es darum, anfällige Assets in der Sicherheitszone des Unternehmens zu finden und Vorschläge zur Optimierung der Sicherheit von Active Directory zu machen.

Das Ziel des Penetrationstests für Active Directory ist die Identifizierung von Schwachstellen im internen Unternehmensnetzwerk.

Der Test umfasst die folgenden Prüfungen:

Netzwerk
- Enumeration und Scan des Domänenservers
- Wiederherstellung der SYSVOL-Struktur und Suche nach Informationen in den GPOs und Skripten
- MITM-Angriffe zum Abgreifen von Kennungen
- Suche nach anonym zugänglichen Fileshares
- passive MITM-Angriffe zum Abgreifen von Authentifizierungsabfragen

Kontenverzeichnis
- Replay von Kennungen aus gestohlenen Datenbanken, die über das Internet zugänglich gemacht wurden
- Suche nach Kennungen in den Metadaten von im Internet veröffentlichten Dateien
- Sammlung von Active-Directory-Gruppen und -Benutzern von gespooftem Konto aus

Kerberos
- Wiederherstellung der Liste der Dienstprinzipalnamen
- Versuch der Entschlüsselung von TGS und ASREP
- Exploit der gefährlichen Kerberos-Delegierung

Domäne
- Identifizierung von Domänen-Controllern
- Exploit von gefährlichen ACLs
- Analyse der Vertrauensstellung

Updates
- Exploit der Abwesenheit eines Patches für das System
- Exploit der Abwesenheit eines Patches für die installierte Software
- Suche nach Software-Schwachstellen für die vom Server bereitgestellten Dienste

Umgehung des Microsoft-Schutzes
- UAC
- SRP
- AppLocker

Konten
- Verzeichnis der Dienstkonten und geplanten Aufgaben
- Wiederherstellung von Authentifizierungsspuren im Speicher des LSASS-Prozesses

LEISTUNGSUMFANG

Der Kunde legt den Umfang des Penetrationstests für Active Directory fest und stellt einen VPN-Zugang zu seinem internen Netzwerk zur Verfügung.

- **Penetrationstest für Active Directory:** Dieser Penetrationstest wird über Remote-VPN innerhalb des betreffenden Unternehmens durchgeführt. Ziel ist in der Regel die Identifizierung und Klassifizierung von Bedrohungen und Schwachstellen im internen Netzwerk, die auf einen bereits bestehenden Zugang zum Unternehmensnetzwerk, beispielsweise durch einen Mitarbeiter, Auftragnehmer oder Gast, zurückzuführen sind.
- Unsere Penetrationstests umfassen Sicherheitsprüfungen, die dazu dienen, negative Auswirkungen auf die Produktionsumgebung des Unternehmens zu begrenzen.

PROZESS DES PENETRATIONSTESTS FÜR ACTIVE DIRECTORY

Ingram Micro nutzt für seine Penetrationstests für Active Directory sowohl automatische als auch manuelle Scanverfahren und arbeitet mit handelsüblichen öffentlichen Tools sowie selbst entwickelten benutzerdefinierten Skripten und Anwendungen.

Der Penetrationstestprozess umfasst die folgenden Schritte:

- **Interne Reconnaissance:** Ausgangspunkt sind die Zugangsrechte des Standardbenutzers. Ziel ist das Aufspüren lokaler Schwachstellen im System, die ausgenutzt werden können, um Zugangsrechte lokaler Administratoren zu erlangen. In dieser Phase werden Informationen über die Active-Directory-Infrastruktur mittels eines Zugangs für nicht zugangsberechtigte Benutzer gesammelt.
- **Administrator-Reconnaissance:** Ist die Enumeration mit dem Standardbenutzer beschränkt, können Administrator Zugangsdaten für die weiteren Schritte der Reconnaissance verwendet werden.
- **Identifizierung der Schwachstellen:** Basierend auf den in den vorherigen beiden Phasen gesammelten Informationen identifizieren wir schwache Dienste in Ihrem Netzwerk oder Anwendungen mit bekannten Schwachstellen.
- **Exploitation:** Wir nutzen bereits verfügbaren Code oder erstellen einen benutzerdefinierten Code, um die identifizierten Schwachstellen zu nutzen und Zugang zu dem betreffenden anfälligen System zu erhalten.
- **Eskalation der Zugangsrechte:** In einigen Fällen bietet die bestehende Schwachstelle nur Zugang auf einer einfachen Ebene, etwa dem normalen Benutzerzugang mit beschränkten Zugangsrechten. In diesem Schritt versuchen wir, einen Zugang mit vollständigen Administratorrechten zu diesem Gerät zu erhalten.
- **Zugangsdaten eines Domänen-Administrators:** Mittels des Zugangs als Domänen-Administrator wird versucht, die Gesamtstruktur-Stammdomäne zu manipulieren und damit das gesamte Active-Directory-Netzwerk des Unternehmens zu beherrschen.

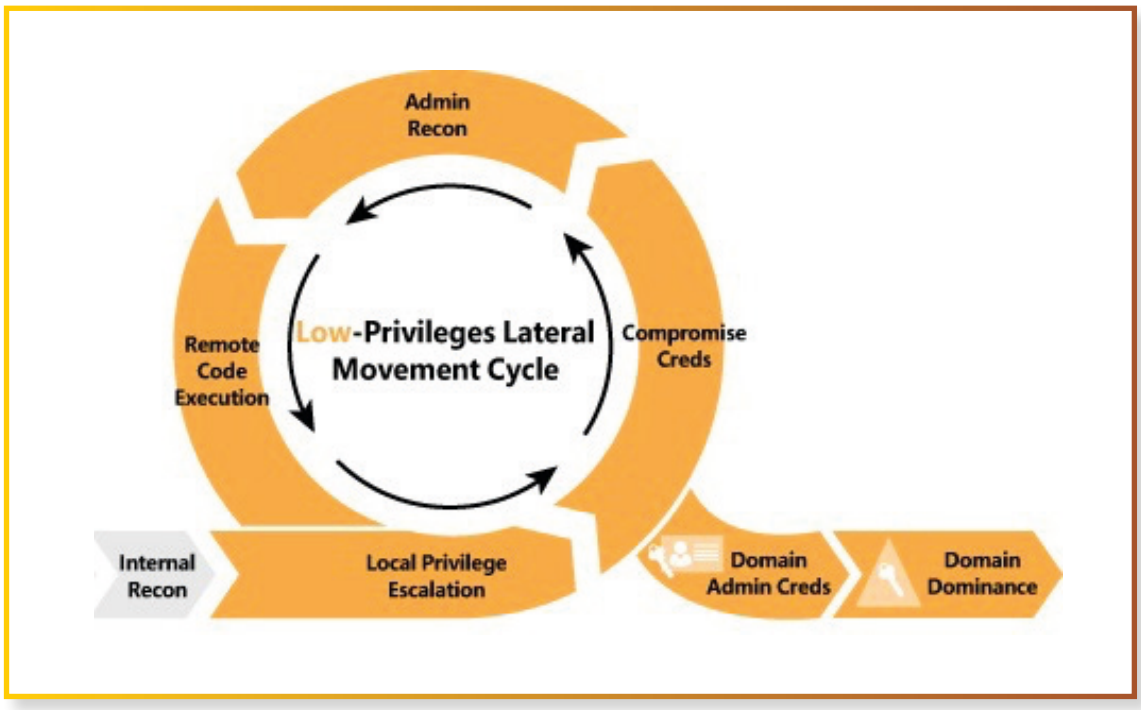


Abbildung 1: Cyber Kill Chain AD-Pentest [https://ptgmedia.pearsoncmg.com]

PROZESS DES PENETRATIONSTESTS FÜR ACTIVE DIRECTORY

Der Kunde stellt Kontaktdaten des Hauptkontakts bereit, der für Ingram Micro während des gesamten Auftrags ansprechbar sein muss. Dieser Vertreter muss ausreichend befugt sein, um Tests zeitlich zu planen und etwaige Probleme zu beheben.

Um den reibungslosen Ablauf der Penetrationstests zu gewährleisten, sind die folgenden Informationen bzw. Vorbereitungen erforderlich:

- VPN-Zugang zum internen Netzwerk
- Zugangsdaten von zwei Benutzern der Domäne
  - **Standardbenutzer:** Wir testen die Eskalation der Zugangsrechte mit den Zugangsrechten eines Standardbenutzers.
  - **Lokaler Administrator:** Ist die lokale Eskalation der Zugangsrechte nicht erfolgreich, werden die Tests mit den Zugangsrechten eines lokalen Administrators durchgeführt

LIEFERGEGENSTÄNDE

Nach Abschluss des externen bzw. internen Penetrationstests erhält der Kunde einen ausführlichen Bericht, der Folgendes enthält:

1. **Allgemeine Zusammenfassung:** Eine Zusammenfassung des Zwecks der Analyse sowie eine kurze Erläuterung der geschäftlichen Bedrohungen, denen das Unternehmen ausgesetzt ist.
2. **Beschreibung der Erkenntnisse:** Eine ausführliche technische Erläuterung der Erkenntnisse der Analyse zusammen mit Schritten und Nachweisen der Erkenntnisse.
3. **Schlussfolgerung und Empfehlungen:** Dieser Abschnitt enthält abschließende Empfehlungen und eine Zusammenfassung der während der Sicherheitsanalyse festgestellten Probleme.

ANNAHMEN

- Der Active-Directory-Penetrationstest wird von den Offshore-Büros von Ingram Micro aus ausgeführt.
- Zugunsten der erfolgreichen Auftragsausführung organisiert der Kunde die erforderlichen Treffen mit den relevanten Interessengruppen.
- Der Kunde muss innerhalb von fünf Geschäftstagen ab Bereitstellung eines Liefergegenstands Rückmeldung dazu abgeben und/oder den Liefergegenstand abzeichnen.
- Der Kunde ist für die Umsetzung der Empfehlungen und/oder der Leitlinien für Korrekturmaßnahmen zuständig.
- Das Team von Ingram Micro konzentriert sich auf die Leitlinien für Korrekturmaßnahmen und delegiert die Schritte an für das Problemmanagement zuständige Team.
- Das Team von Ingram Micro ist nicht für die Behebung bzw. Minderung von im Rahmen der Penetrationstests festgestellten Schwachstellen zuständig. Der Leistungsumfang des Auftrags ist auf Penetrationstätigkeiten bzw. Leitlinien für Korrekturmaßnamen beschränkt.

Penetrationstest für Web Anwendungen

Ziel des Penetrationstests für Web Anwendungen ist, das Schutzkonzept von Web Anwendungen zu analysieren, indem Schwachstellen in Design und Implementierung identifiziert und geprüft werden. Dabei wird mittels automatisierter und manueller Tools die Wirksamkeit der Schutzmechanismen, z. B. der Firewalls der Web Anwendungen (Web Application Firewalls, WAF), überprüft.

Unsere Methodik gründet u.a. auf den folgenden Branchenstandards:

- Penetration Testing Execution Standard (PTES)
- Open Web Application Security Project (OWASP) Testing Guide
- Open-Source Security Testing Methodology Manual (OSSTMM)

LEISTUNGSUMFANG

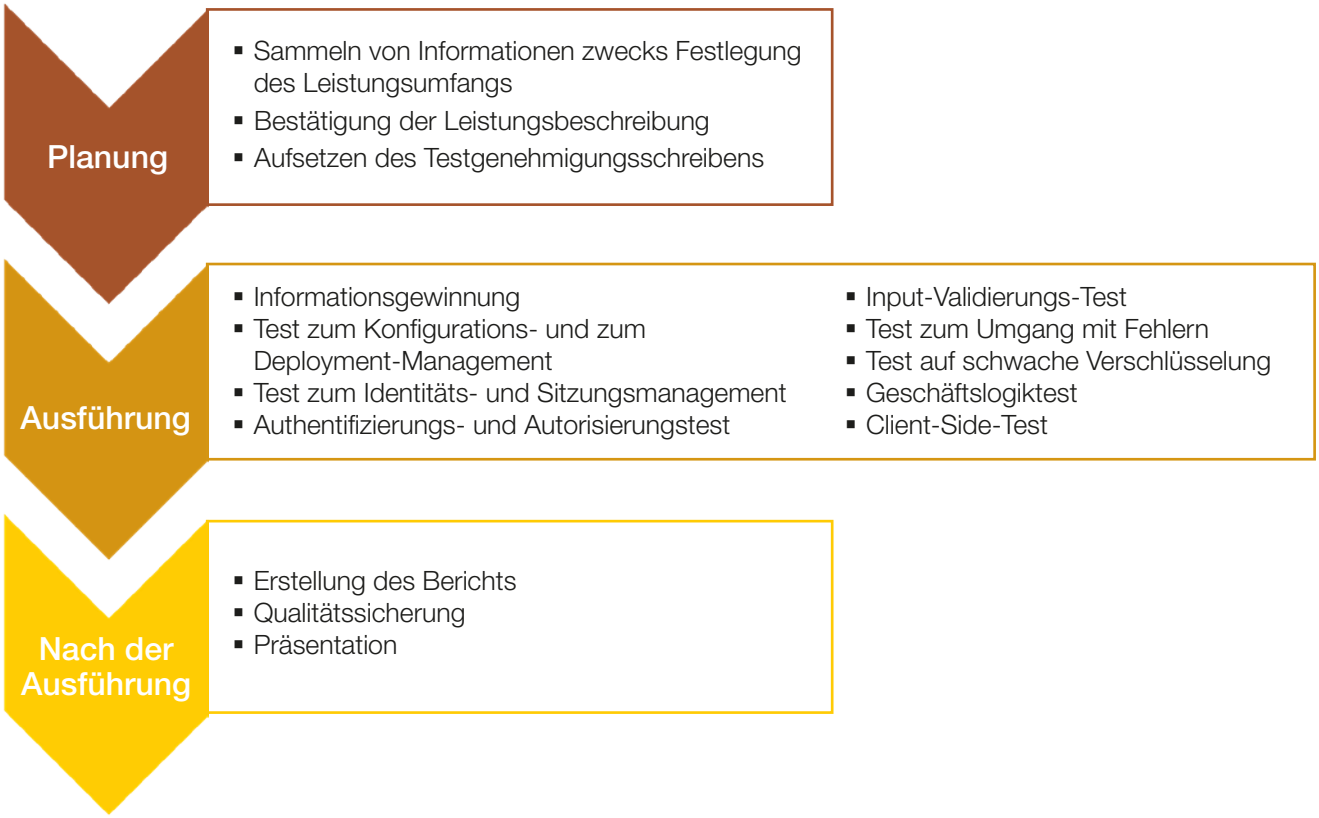
Im Rahmen des Penetrationstests für Web Anwendungen werden Anwendungen analysiert und manipuliert. Dabei kommen verschiedene Mittel und Techniken zum Einsatz, wie sie auch von echten Angreifern genutzt werden.
Vorgegangen wird nach der OWASP-Methode und dem OWASP-Leitfaden. Die Tests können sowohl authentifiziert als auch nicht authentifiziert durchgeführt werden. In beiden Szenarien versucht unser Testteam eine Eskalation der Zugangsrechte, um sich Zugang zu zugangsbeschränkten Daten zu verschaffen. In bestimmten Fällen kann der Test auch auf die den Web Anwendungen zugrundeliegende Infrastruktur zielen, um die Hosting-Instanz zu stärken und das interne Netzwerk zu optimieren.
Zwar werden auch automatisierte Scans durchgeführt, der Großteil des Auftrags wird jedoch manuell mittels kundenspezifischer Payloads zur Funktionsanalyse und Defence Evasion ausgeführt.

GRENZEN DES LEISTUNGSUMFANGS

Das Folgende ist NICHT Bestandteil dieses Angebots:

- Implementierung von Maßnahmen und Empfehlungen zur Risikominderung
- Sicherheitshärtung, Behebung von Schwachstellen, Patching und Entwicklung von Modulen zur Risikominderung
- Denial-of-Service-Test und -Exploit
- Social Engineering und Client-Side-Angriffe
- sämtliche Tätigkeiten, die nicht ausdrücklich in dieser Dienstleistungsbeschreibung niedergelegt sind

UNSER DIENSTLEISTUNGSPROZESS



PLANUNG

Die Planungsphase ist entscheidend für den Erfolg des Auftrags. In dieser Phase werden die für die Analyse erforderlichen Informationen zusammengetragen. Dazu zählen Informationen zu u. a. den zu testenden IT-Komponenten, den relevanten Bedrohungen für diese Komponenten sowie den im Analyseansatz zur Risikominderung anzuwendenden Sicherheitskontrollen. Eine Sicherheitsanalyse erfolgt wie jedes andere Projekt auf der Grundlage eines Projektmanagementplans, in dem die Ziele und Ergebnisse, der Leistungsumfang, die Anforderungen, die Rollen und Zuständigkeiten sowie die Grenzen, Erfolgsfaktoren, Annahmen, Ressourcen, zeitliche Planung und Liefergegenstände niedergelegt sind.

Nach dem Projektstart werden die Anforderungen des Kunden erhoben, auf deren Grundlage Ingram Micro einen Entwurf für die Leistungsbeschreibung aufsetzt. Nach Einigung über die Bestimmungen der Leistungsbeschreibung wird der Leistungsumfang umfassend spezifiziert. Dies beinhaltet das Aufsetzen und die Unterzeichnung des Testgenehmigungsschreibens durch beide Parteien sowie eine kurze Besprechung zur Endabstimmung der zeitlichen Planung und Kommunikationsdetails. Das Testgenehmigungsschreiben dient der Bestätigung der Auftragsbedingungen und der Beantwortung aller Fragen vor dem Projektbeginn.

PENETRATIONSTEST FÜR WEB ANWENDUNGEN – METHODIK

Der Penetrationstest von Ingram Micro zielt auf die Identifizierung von Schwachstellen, die gemäß Open Web Application Security Project (OWASP) zu den zehn nachstehend aufgeführten wichtigsten Sicherheitsrisiken für Web Anwendungen zählen.

1. Injection-Lücken

Injection-Lücken, z. B. in Form von SQL-, NoSQL-, OS- und LDAP-Injection, entstehen, wenn nicht vertrauenswürdige Daten im Rahmen eines Befehls oder einer Abfrage an einen Interpreter gesendet werden. Die schädlichen Daten des Angreifers können den Interpreter dazu veranlassen, unbeabsichtigte Befehle auszuführen oder unbefugt auf Daten zuzugreifen.

2. Fehler bei der Authentifizierung

Anwendungsfunktionen für Authentifizierung und Sitzungsmanagement sind oftmals fehlerhaft implementiert. Dadurch können Angreifer Passwörter, Schlüssel oder Sitzungs-Tokens manipulieren oder andere Implementierungsschwächen ausnutzen und vorübergehend oder dauerhaft Benutzeridentitäten übernehmen.

3. Offenlegung sensibler Daten

Viele Web Anwendungen und APIs schützen sensible Daten, etwa Finanz-, Gesundheits- oder persönlich identifizierende Daten, nur unzureichend. Angreifer können diese schlecht geschützten Daten stehlen oder verändern und damit Kreditkartenbetrug, Identitätsdiebstahl oder andere Straftaten begehen. Ohne besondere Absicherung (z. B. durch Verschlüsslung) sind sensible Daten sowohl at rest als auch in transit nicht ausreichend geschützt. Besondere Vorsicht ist auch beim Datenaustausch mit Browsern geboten.

4. Externe XML-Entitäten (XXE)

Viele ältere oder schlecht konfigurierte XML-Prozessoren evaluieren externe Entitätsreferenzen in XML-Dokumenten. Externe Entitäten können über URI-Handler, interne Fileshares, interne Port-Scans, Remote-Code-Ausführung und Denial-of-Service-Angriffe zur Offenlegung interner Dateien verwendet werden.

5. Fehler bei der Zugangskontrolle

Zugangsbeschränkungen für authentifizierte Benutzer werden oftmals nicht konsequent umgesetzt. Angreifer können diese Schwachstelle ausnutzen, um sich u.a. unbefugt Zugang zu Funktionen und/oder Daten wie etwa Benutzerkonten oder sensiblen Dateien zu verschaffen oder um Benutzerdaten oder Zugangsrechte zu verändern.

6. Sicherheitsfehlkonfiguration

Die Sicherheitsfehlkonfiguration gehört zu den häufigsten Sicherheitsmängeln. Sie resultiert oftmals aus unsicheren Standardkonfigurationen, unvollständigen oder Ad-hoc-Konfigurationen, Open-Cloud-Storage, fehlkonfigurierten HTTP-Headern und umfangreichen Fehlermeldungen, die sensible Daten enthalten. Sämtliche Betriebssysteme, Frameworks, Bibliotheken und Anwendungen müssen nicht nur sicher konfiguriert sein, sondern auch durch Patches bzw. Upgrades gesichert werden.

7. Cross-Site-Scripting (XSS)

XSS-Lücken entstehen, wenn über eine Anwendung aufgrund von mangelnder Überprüfung oder mangelhaftem Escaping nicht vertrauenswürdige Daten in eine neue Webseite eingefügt werden oder eine bestehende Webseite mit benutzerseitig bereitgestellten Daten aktualisiert wird und dabei eine Browser-API verwendet wird, die HTML oder JavaScript generieren kann. Mittels XXS können Angreifer Skripte im Browser des Opfers ausführen und dadurch Benutzersitzungen entführen, Website-Defacements durchführen und den Benutzer zu Schadseiten weiterleiten.

8. Unsichere Deserialisierung

Folge der unsicheren Deserialisierung ist oftmals die Remote-Code-Ausführung. Selbst wenn es nicht dazu kommt, können Schwachstellen bei der Deserialisierung für Angriffe missbraucht werden, z. B. für Replay-Angriffe, Injection-Angriffe und Angriffe zur Eskalation der Zugangsrechte.

9. Nutzung von Komponenten mit bekannten Schwachstellen

Komponenten wie Bibliotheken, Frameworks oder andere Softwaremodule laufen mit denselben Zugangsrechten wie die Anwendung. Angriffe auf solche anfälligen Komponenten können erhebliche Datenverluste oder Server-Übernahmen zur Folge haben. Anwendungen und APIs, die Komponenten mit bekannten Schwachstellen nutzen, schwächen den Anwendungsschutz und bieten Angriffsflächen – mit mitunter schwerwiegenden Folgen.

10. Unzureichendes Logging und Monitoring

Unzureichendes Logging und Monitoring ermöglicht Angreifern insbesondere bei fehlender oder mangelhafter Integration in die Incident Response weitreichende, dauerhafte Angriffe auf Systeme, den Übergriff auf andere Systeme und die Veränderung, Extraktion oder Vernichtung von Daten. Die meisten Studien zu Sicherheitslücken zeigen, dass in der Regel über 200 Tage vergehen, bis eine Sicherheitslücke entdeckt wird, und zwar meist von Externen und nicht durch interne Prozesse oder Überwachung.

TOOLS

Ingram Micro verwendet sowohl branchenübliche Tools und Frameworks als auch unsere eigenen Skripte. Auf diese Weise gewährleisten wir, dass unsere Penetrationstests möglichst lückenlos und umfassend ist.

Bei unseren Penetrationstests setzen wir u. a. die folgenden Tools ein:

- Burp Suite Pro
- OWASP Zap
- Dirbuster/Dirb/GoBuster
- Wfuzz/ffuf
- Nikto
- Nuclei
- Sqlmap
- Hydra
- Nmap
- Nessus Professional
- Metasploit Framework
- Custom Scripts

NACH DER AUSFÜHRUNG

Nach dem Abschluss der Ausführungsphase dokumentiert Ingram Micro alle Erkenntnisse in einem Bericht. Dieser Bericht wird zunächst der internen Qualitätssicherung unterzogen, bevor der Abschlussbericht innerhalb von zwei Wochen nach Auftragsabschluss an den Kunden übermittelt wird.
Dieser Bericht rundet den Auftrag ab und besteht aus einer allgemeinen Zusammenfassung, die als Grundlage für strategische Unternehmensentscheidungen dienen kann, sowie auf einer ausführlichen Analysebeschreibung, anhand derer sich die technischen Aspekte der Tests nachvollziehen lassen.

Der Bericht gliedert sich in die folgenden Abschnitte:

- Allgemeine Zusammenfassung
- Technische Zusammenfassung
- Analysebeschreibung
- Erkenntnisse
- Anhänge (mit Scanergebnissen und Erläuterungen zur Methodik)

ÜBERPRÜFUNG DER ERGRIFFENEN KORREKTURMASSNAHMEN

Falls das Unternehmen die Korrekturmaßnahmen, die zur Behebung der ermittelten Schwachstellen unternommen wurden, überprüfen möchte, führt Ingram Micro diese Überprüfung gerne gegen Aufpreis durch.
Für weitere Informationen und die zeitliche Planung steht Ihnen Ihr Channel-Partner gerne zur Verfügung.

PFLICHTEN DES KUNDEN

Der Kunde verpflichtet sich zur Erfüllung seiner Pflichten und erkennt an und erklärt sich damit einverstanden, dass **die Erfüllung der Pflichten von Ingram Micro von dem Folgenden abhängt:**

- Die Ressourcen des Kunden stehen Ingram Micro plangemäß zur Verfügung.
- Alle zu analysierenden Server und Netzwerke sind bei Durchführung der Analyse in Betrieb und funktionsfähig.
- Der Kunde stellt sämtliche angefragten Dokumente und Informationen rechtzeitig und im Einklang mit den in der Planungsphase festgelegten Lieferterminen zur Verfügung.
- Zu Testzwecken wird jede im Leistungsumfang enthaltene IP als separater Host betrachtet, und zwar unabhängig vom potenziellen Lastenausgleich, von Firewalls usw.
- Sofern keine anderweitigen Bedingungen mit dem Unternehmen vereinbart wurden, werden sämtliche Test- und Analysetätigkeiten in einem Zeitfenster von 24 Stunden durchgeführt.
- Die Testzeitfenster des Kunden müssen lange genug für die Durchführung der Tätigkeiten sein.

Es gelten die vor Ort anwendbaren Allgemeine Geschäftsbedingungen von Ingram Micro.

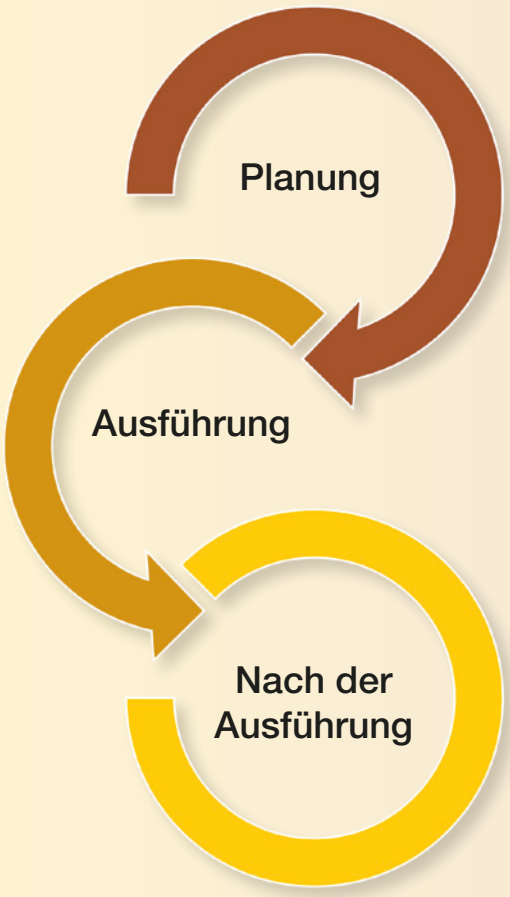
Penetrationstest für APIs

PENETRATIONSTEST FÜR APIs

Mit Penetrationstests für Application Programming Interfaces (APIs) wird das Sicherheitskonzept von Umgebungen, die APIs nutzen und die Übertragung von Daten erfordern, überprüft. Im Rahmen des Auftrags wird die Anwendungslogik untergraben, sodass sensible Daten durch den Zugang zu zugangsbeschränkten Funktionen und Zugangsebenen offengelegt werden. Für den Test werden überwiegend manuelle Techniken der Enumeration und Exploitation im Einklang mit dem OWASP API Testing Guide angewandt.

Unsere Methodik gründet u.a. auf den folgenden Branchenstandards:

- Penetration Testing Execution Standard (PTES)
- Open Web Application Security Project (OWASP) Testing Guide
- Open-Source Security Testing Methodology Manual (OSSTMM)



- Sammeln von Informationen zwecks Festlegung des Leistungsumfangs
- Bestätigung der Leistungsbeschreibung
- Aufsetzen des Testgenehmigungsschreibens

- Informationsgewinnung
- Listung und Enumeration der Endpunkte
- Test zu Abfragemethoden
- Test auf Basis des Leistungsumfangs
- Rollenbasierter Test
- Test zu Insecure Direct Object Reference (IDOR)

- Erstellung des Berichts
- Qualitätssicherung
- Präsentation

LEISTUNGSUMFANG

Mit dem Penetrationstest für APIs wird das Gesamtrisiko für die API-Kommunikation analysiert, indem umfassende Informationen zur Anwendungslogik gewonnen werden und auf Grundlage dieser Informationen das Verhalten der Anwendung manipuliert wird. Geprüft werden verschiedene Plattformen, von klassischen REST- und SOAP-basierten APIS bis hin zu GraphQL und kundenspezifischen Implementierungen. Zugunsten einer tiefgehenden, umfassenden Analyse ist eine Dokumentation mit API-Funktion- und Beispielaufrufen erforderlich.

GRENZEN DES LEISTUNGSUMFANGS

Das Folgende ist NICHT Bestandteil dieses Angebots:

- Implementierung von Maßnahmen und Empfehlungen zur Risikominderung
- Sicherheitshärtung, Behebung von Schwachstellen, Patching und Entwicklung von Modulen zur Risikominderung
- Denial-of-Service-Test und -Exploit
- Social Engineering und Client-Side-Angriffe
- sämtliche Tätigkeiten, die nicht ausdrücklich in dieser Dienstleistungsbeschreibung niedergelegt sind

PLANUNG

Die Planungsphase ist entscheidend für den Erfolg des Auftrags. In dieser Phase werden die für die Analyse erforderlichen Informationen zusammengetragen. Dazu zählen Informationen zu u. a. den zu testenden IT-Komponenten, den relevanten Bedrohungen für diese Komponenten, etwaigen relevanten Dokumentationen sowie den im Analyseansatz zur Risikominderung anzuwendenden Sicherheitskontrollen.
Eine Sicherheitsanalyse erfolgt wie jedes andere Projekt auf der Grundlage eines Projektmanagementplans, in dem die Ziele und Ergebnisse, der Leistungsumfang, die Anforderungen, die Rollen und Zuständigkeiten sowie die Grenzen, Erfolgsfaktoren, Annahmen, Ressourcen, zeitliche Planung und Liefergegenstände niedergelegt sind.

Nach dem Projektstart werden die Anforderungen des Kunden erhoben, auf deren Grundlage Ingram Micro einen Entwurf für die Leistungsbeschreibung aufsetzt. Nach Einigung über die Bestimmungen der Leistungsbeschreibung wird der Leistungsumfang umfassend spezifiziert. Dies beinhaltet das Aufsetzen und die Unterzeichnung des Testgenehmigungsschreibens durch beide Parteien sowie eine kurze Besprechung zur Endabstimmung der zeitlichen Planung und Kommunikationsdetails. Das Testgenehmigungsschreiben dient der Bestätigung der Auftragsbedingungen und der Beantwortung aller Fragen vor dem Projektbeginn.

PENETRATIONSTEST FÜR APIs – METHODIK

Der Penetrationstest von Ingram Micro zielt auf die Identifizierung von Schwachstellen, die gemäß Open Web Application Security Project (OWASP) zu den zehn nachstehend aufgeführten wichtigsten Sicherheitsrisiken für APIs zählen.

1. Fehler bei der Autorisierung auf Objektebene
APIs verfügen tendenziell über Endpunkte, die mit Objektkennungen arbeiten. Deshalb bieten sie eine gute Angriffsfläche im Bereich der Zugangskontrolle. Autorisierungsprüfungen auf Objektebene sollten für jede Funktion durchgeführt werden, die durch Zutun des Benutzers auf eine Datenquelle zugreift.

2. Fehler bei der Benutzerauthentifizierung
Mechanismen der Authentifizierung sind oftmals fehlerhaft implementiert. Dadurch können Angreifer Authentifizierungs-Tokens manipulieren oder andere Implementierungsschwächen ausnutzen und vorübergehend oder dauerhaft Benutzeridentitäten übernehmen. Ist das System nicht mehr in der Lage, den Client/Benutzer zu erkennen, schwächt das die API-Sicherheit insgesamt.

3. Übermäßige Offenlegung von Daten
Mit Blick auf generische Implementierungen tendieren Entwickler dazu, alle Objekteigenschaften – ob sensibel oder nicht – offenzulegen und es dem Kunden zu überlassen, die Daten zu filtern, bevor sie dem Benutzer angezeigt werden.

4. Ressourcenmangel und Durchsatzratenbegrenzung
Oftmals weisen APIs hinsichtlich der Größe oder Anzahl der Ressourcen, die vom Kunden bzw. Benutzer abgefragt werden können, keinerlei Beschränkungen auf. Dies kann nicht nur die API-Serverleistung beeinträchtigen mit der Folge eines Denial-of-Service (DoS), sondern ermöglicht auch Sicherheitslücken, die beispielsweise für Brute-Force-Angriffe ausgenutzt werden können.

5. Fehler bei der Autorisierung auf Funktionsebene
Komplexe Konzepte der Zugangskontrolle, die mit verschiedenen Hierarchien, Gruppen und Rollen arbeiten und in denen nicht sauber zwischen administrativen und regulären Funktionen getrennt wird, sind fehleranfällig. Angreifer nutzen diese Fehler aus und verschaffen sich Zugang zu den Ressourcen und/oder Verwaltungsfunktionen der Benutzer.

6. Massenzuweisung
Wenn vom Kunden bereitgestellte Daten (z. B. JSON) an Datensatzmuster geknüpft werden, ohne dass eine angemessene Filterung nach Eigenschaften auf der Grundlage einer Positivliste erfolgt, kommt es in der Regel zu einer Massenzuweisung. Dadurch können Angreifer Objekteigenschaften ableiten, andere API-Endpunkte auskundschaften, Dokumentation lesen oder weitere Objekteigenschaften aus Request-Payloads entnehmen, um dann unbefugt Objekteigenschaften zu ändern.

7. Sicherheitsfehlkonfiguration
Sie resultiert oftmals auch unsicheren Standardkonfigurationen, unvollständigen oder Ad-hoc-Konfigurationen, Open-Cloud-Storage, fehlkonfigurierten HTTP-Headern, unnötigen HTTP-Methoden, großzügigem Cross-Origin-Resource-Sharing (CORS) und umfangreichen Fehlermeldungen, die sensible Daten enthalten.

8. Injection-Lücken
Injection-Lücken, z. B. in Form von SQL-, NoSQL- oder Command-Injection, entstehen, wenn nicht vertrauenswürdige Daten im Rahmen eines Befehls oder einer Abfrage an einen Interpreter gesendet werden. Die schädlichen Daten des Angreifers können den Interpreter dazu veranlassen, fälschlicherweise unbeabsichtigte Befehle auszuführen oder unbefugt auf Daten zuzugreifen.

9. Mangelhaftes Asset-Management
APIs haben oftmals mehr Endpunkte als klassische Web Anwendungen. Besonders wichtig ist daher die ordnungsgemäße, laufende Dokumentation. Gute Hosts und das Inventar von API-Versionen spielen ebenfalls eine wichtige Rolle, um zu vermeiden, dass etwa API-Versionen veraltet oder Debug-Endpunkte frei zugänglich sind.

10. Unzureichendes Logging und Monitoring
Unzureichendes Logging und Monitoring ermöglicht Angreifern insbesondere bei fehlender oder mangelhafter Integration in die Incident Response weitreichende, dauerhafte Angriffe auf Systeme, den Übergriff auf andere Systeme und die Veränderung, Extraktion oder Vernichtung von Daten. Die meisten Studien zu Sicherheitslücken zeigen, dass in der Regel über 200 Tage vergehen, bis eine Sicherheitslücke entdeckt wird, und zwar meist von Externen und nicht durch interne Prozesse oder Überwachung.

TOOLS

Ingram Micro verwendet sowohl branchenübliche Tools und Frameworks als auch unsere eigenen Skripte. Auf diese Weise gewährleisten wir, dass unsere Penetrationstests möglichst lückenlos und umfassend ist.

Bei unseren Penetrationstests setzen wir u. a. die folgenden Tools ein:

- Burp Suite Pro
- OWASP Zap
- Postman
- SoapUI
- WSDLer
- Astra
- curl
- Dirbuster/Dirb/GoBuster
- Wfuzz/ffuf
- Nikto
- Sqlmap
- Custom Scripts

NACH DER AUSFÜHRUNG

Nach dem Abschluss der Ausführungsphase dokumentiert Ingram Micro alle Erkenntnisse in einem Bericht. Dieser Bericht wird zunächst der internen Qualitätssicherung unterzogen, bevor der Abschlussbericht innerhalb von zwei Wochen nach Auftragsabschluss an den Kunden übermittelt wird.
Dieser Bericht rundet den Auftrag ab und besteht aus einer allgemeinen Zusammenfassung, die als Grundlage für strategische Unternehmensentscheidungen dienen kann, sowie auf einer ausführlichen Analysebeschreibung, anhand derer sich die technischen Aspekte der Tests nachvollziehen lassen.

Der Bericht gliedert sich in die folgenden Abschnitte:

- Allgemeine Zusammenfassung
- Technische Zusammenfassung
- Analysebeschreibung
- Erkenntnisse
- Anhänge (mit Scanergebnissen und Erläuterungen zur Methodik)

ÜBERPRÜFUNG DER ERGRIFFENEN KORREKTURMASSNAHMEN

Falls das Unternehmen die Korrekturmaßnahmen, die zur Behebung der ermittelten Schwachstellen unternommen wurden, überprüfen möchte, führt Ingram Micro diese Überprüfung gerne gegen Aufpreis durch.
Für weitere Informationen und die zeitliche Planung steht Ihnen Ihr Channel-Partner gerne zur Verfügung.

PFLICHTEN DES KUNDEN

Der Kunde verpflichtet sich zur Erfüllung seiner Pflichten und erkennt an und erklärt sich damit einverstanden, dass **die Erfüllung der Pflichten von Ingram Micro von dem Folgenden abhängt:**

- Die Ressourcen des Kunden stehen Ingram Micro plangemäß zur Verfügung.
- Alle zu analysierenden Server und Netzwerke sind bei Durchführung der Analyse in Betrieb und funktionsfähig.
- Der Kunde stellt sämtliche angefragten Dokumente und Informationen rechtzeitig und im Einklang mit den in der Planungsphase festgelegten Lieferterminen zur Verfügung.
- Zu Testzwecken wird jede im Leistungsumfang enthaltene IP als separater Host betrachtet, und zwar unabhängig vom potenziellen Lastenausgleich, von Firewalls usw.
- Sofern keine anderweitigen Bedingungen mit dem Unternehmen vereinbart wurden, werden sämtliche Test- und Analysetätigkeiten in einem Zeitfenster von 24 Stunden durchgeführt.
- Die Testzeitfenster des Kunden müssen lange genug für die Durchführung der Tätigkeiten sein.

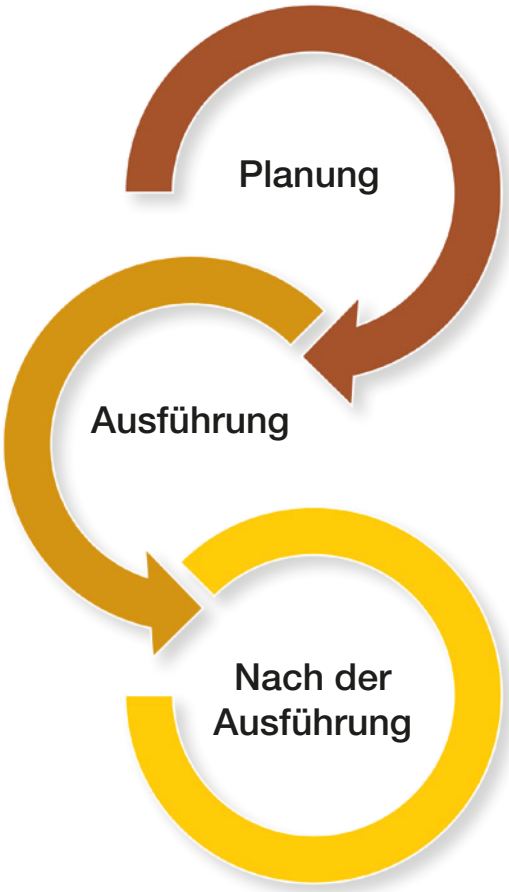
Es gelten die vor Ort anwendbaren Allgemeine Geschäftsbedingungen von Ingram Micro.

Schwachstellenanalyse

Die Schwachstellenanalyse zielt auf die Identifizierung, Klassifikation und Priorisierung von Schwachstellen in Netzwerken, Datenbanken und Anwendungen. Dieser Auftrag ist umfangreicher und komplexer als einfache Scans, da er auch individuelle Tests auf Non-Compliance und Fehlkonfigurationen für die Instanzen der Umgebung des Kunden umfasst. Auf der Grundlage der gewonnenen Informationen werden die Schwachstellen nach ihrem Kontext klassifiziert und anhand bewährter, branchenüblicher Verfahren des Risikomanagements priorisiert.

Je nach Auftrag werden die folgenden Arten von Schwachstellenanalysen durchgeführt:

- Netzwerk- und Drahtlosnetzwerkanalysen
- Host-Analysen
- Datenbankanalysen
- Anwendungsscans



- Sammeln von Informationen zwecks Festlegung des Leistungsumfangs
- Bestätigung der Leistungsbeschreibung
- Aufsetzen des Testgenehmigungsschreibens

- automatisierte Scans
- manuelle Validierung
- Risikobewertung und -priorisierung

- Erstellung des Berichts
- Qualitätssicherung
- Präsentation

LEISTUNGSUMFANG

Bei Schwachstellenanalyse werden Schwachstellen identifiziert und dokumentiert. Dabei wird auf einen aktiven Exploit verzichtet. Vielmehr liegt der Fokus auf passiven und aktiven Scanning-Methoden, mittels derer Schwachstellen in den betreffenden Netzwerken und Systemen aufgezeigt werden.
Der aktive Exploit erfolgt im Rahmen des Penetrationstests. Informationen zu einer möglichen Validierung der identifizierten Elemente finden sich in diesem Dokument im Abschnitt zu unseren Penetrationstests.

GRENZEN DES LEISTUNGSUMFANGS

Das Folgende ist NICHT Bestandteil dieses Angebots:

- Implementierung von Maßnahmen und Empfehlungen zur Risikominderung
- Sicherheitshärtung, Behebung von Schwachstellen, Patching und Entwicklung von Modulen zur Risikominderung
- aktives Exploit für identifizierte Schwachstellen
- Denial-of-Service-Test
- sämtliche Tätigkeiten, die nicht ausdrücklich in dieser Dienstleistungsbeschreibung niedergelegt sind

PLANUNG

Die Planungsphase ist entscheidend für den Erfolg des Auftrags. In dieser Phase werden die für die Analyse erforderlichen Informationen zusammengetragen. Dazu zählen Informationen zu u. a. den zu testenden IT-Komponenten, den relevanten Bedrohungen für diese Komponenten sowie den im Analyseansatz zur Risikominderung anzuwendenden Sicherheitskontrollen. Eine Sicherheitsanalyse erfolgt wie jedes andere Projekt auf der Grundlage eines Projektmanagementplans, in dem die Ziele und Ergebnisse, der Leistungsumfang, die Anforderungen, die Rollen und Zuständigkeiten sowie die Grenzen, Erfolgsfaktoren, Annahmen, Ressourcen, zeitliche Planung und Liefergegenstände niedergelegt sind.

Nach dem Projektstart werden die Anforderungen des Kunden erhoben, auf deren Grundlage Ingram Micro einen Entwurf für die Leistungsbeschreibung aufsetzt. Nach Einigung über die Bestimmungen der Leistungsbeschreibung wird der Leistungsumfang umfassend spezifiziert. Dies beinhaltet das Aufsetzen und die Unterzeichnung des Testgenehmigungsschreibens durch beide Parteien sowie eine kurze Besprechung zur Endabstimmung der zeitlichen Planung und Kommunikationsdetails. Das Testgenehmigungsschreiben dient der Bestätigung der Auftragsbedingungen und der Beantwortung aller Fragen vor dem Projektbeginn.

SCHWACHSTELLENANALYSE – METHODIK

Die Schwachstellenanalyse von Ingram Micro verzichtet auf detaillierte Netzwerk- oder Infrastrukturdiagramme sowie auf Konten oder zusätzliche Benutzerinformationen, es sei denn, diese sind laut Leistungsumfang vorgesehen. Bei Bedarf können aber auch Scans aus der Grundlage von Benutzerdaten durchgeführt werden.

Wir arbeiten mit den folgenden Methoden:

- **Automatisierte Scans**
  Scans unter Verwendung verschiedener Tools
- **Manuelle Validierung**
  Verifizierung mittels manueller Prüfungen zwecks Vermeidung von falsch positiven Ergebnissen
- **Risikobewertung und -priorisierung**
  Dokumentation der ermittelten Sicherheitsprobleme

Ingram Micro verwendet sowohl branchenübliche Tools und Frameworks als auch unsere eigenen Skripte. Auf diese Weise gewährleisten wir, dass unsere Schwachstellenanalyse möglichst lückenlos und umfassend ist.

Bei unseren Penetrationstests setzen wir u. a. die folgenden Tools ein:

- Nessus Professional
- Netsparker
- Testssl.sh
- Burp Suite Pro
- Nikto
- Sqlmap
- Metasploit Framework
- Custom Scripts

NACH DER AUSFÜHRUNG

Nach dem Abschluss der Ausführungsphase dokumentiert Ingram Micro alle Erkenntnisse. Dieser Bericht wird zunächst der internen Qualitätssicherung unterzogen, bevor der Abschlussbericht innerhalb von zwei Wochen nach Auftragsabschluss an den Kunden übermittelt wird.
Dieser Bericht rundet den Auftrag ab und besteht aus einer ausführlichen Übersicht der identifizierten Schwachstellen sowie Empfehlungen für Korrekturmaßnahmen.

ÜBERPRÜFUNG DER ERGRIFFENEN KORREKTURMASSNAHMEN

Falls das Unternehmen die Korrekturmaßnahmen, die zur Behebung der ermittelten Schwachstellen unternommen wurden, überprüfen möchte, führt Ingram Micro diese Überprüfung gerne gegen Aufpreis durch.
Für weitere Informationen und die zeitliche Planung steht Ihnen Ihr Channel-Partner gerne zur Verfügung.

PFLICHTEN DES KUNDEN

Der Kunde verpflichtet sich zur Erfüllung seiner Pflichten und erkennt an und erklärt sich damit einverstanden, dass **die Erfüllung der Pflichten von Ingram Micro von dem Folgenden abhängt:**

- Die Ressourcen des Kunden stehen Ingram Micro plangemäß zur Verfügung.
- Alle zu analysierenden Server und Netzwerke sind bei Durchführung der Analyse in Betrieb und funktionsfähig.
- Der Kunde stellt sämtliche angefragten Dokumente und Informationen rechtzeitig und im Einklang mit den in der Planungsphase festgelegten Lieferterminen zur Verfügung.
- Zu Testzwecken wird jede im Leistungsumfang enthaltene IP als separater Host betrachtet, und zwar unabhängig vom potenziellen Lastenausgleich, von Firewalls usw.
- Sofern keine anderweitigen Bedingungen mit dem Unternehmen vereinbart wurden, werden sämtliche Test- und Analysetätigkeiten in einem Zeitfenster von 24 Stunden durchgeführt.
- Die Testzeitfenster des Kunden müssen lange genug für die Durchführung der Tätigkeiten sein.

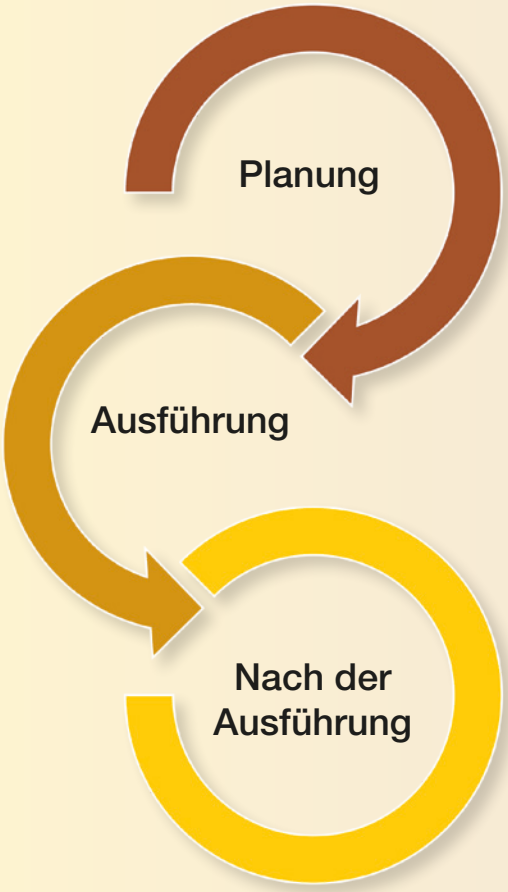
Es gelten die vor Ort anwendbaren Allgemeine Geschäftsbedingungen von Ingram Micro.

Penetrationstest für mobile Anwendungen

Mit Penetrationstests für Application Programming Interfaces (APIs) wird das Sicherheitskonzept von Umge-
Zweck des Penetrationstests für mobile Anwendungen ist die Identifizierung von Sicherheitslücken in den mobilen Android- und iOS-Anwendungen des Kunden. Ingram Micro prüft die Sicherheit der Anwendungen mittels statischer und dynamischer Analyse im Einklang mit dem Prüfleitfaden von Open Web Application Security Project (OWASP). Unsere Methodik gründet u. a. auf den folgenden Branchenstandards:

Unsere Methodik gründet u.a. auf den folgenden Branchenstandards:

- Penetration Testing Execution Standard (PTES)
- Open Web Application Security Project (OWASP) Testing Guide
- The OWASP Mobile Application Security Verification Standard (MASVS)
- OWASP Mobile Application Security Checklist



- Sammeln von Informationen zwecks Festlegung des Leistungsumfangs
- Bestätigung der Leistungsbeschreibung
- Aufsetzen des Testgenehmigungsschreibens

- Identifizierung von sensiblen Daten und Anwendungs-Mapping
- Bewertung von Datenspeicherung und Datenschutz
- Authentifizierungs- und Autorisierungstest
- Test auf schwache Verschlüsselung
- Prüfung der Code-Qualität
- Tampering und Reverse Engineering

- Erstellung des Berichts
- Qualitätssicherung
- Präsentation

LEISTUNGSUMFANG

Penetrationstests für mobile Anwendungen zielen darauf, Anwendungen zu dekompilieren und herauszufinden, wie sie geschrieben sind, wie sie mit der Geräteplattform interagieren, wie sie mit serverseitigen Systemen kommunizieren und wie sicher sie in die Umgebung des Kunden und seines Unternehmens integriert sind. Dabei wird auch analysiert, welche Netzwerkprotokolle genutzt werden, wird eine Log-Analyse durchgeführt und werden die vorhandenen Verfahren der Verschlüsselung und Datenspeicherung untersucht.

Ingram Micro bietet drei Ansätze für Penetrationstests für mobile Anwendungen:

- **White-Box**
  Dieser Ansatz eignet sich für kurzfristigere, sehr dringende Aufträge. Wenn wir über den Quellcode für die im Leistungsumfang enthaltenen Anwendungen verfügen, spart dies Zeit, da dann die Notwendigkeit für Reverse Engineering und Deobfuscation entfallen.
- **Black-Box**
  Sämtliche Tätigkeiten werden ohne Kenntnis der im Leistungsumfang enthaltenen Anwendung(en) durchgeführt. Zweck ist die Simulation eines echten Angriffs aus dem öffentlichen Raum. Gute Ergebnisse brauchen Zeit. Daher ist der Zeitaufwand für diesen Auftrag möglicherweise höher.
- **Grey-Box**
  Dieser Ansatz verbindet die beiden anderen Ansätze. In diesem Szenario erhält das Testteam nur begrenzt Informationen.

GRENZEN DES LEISTUNGSUMFANGS

Das Folgende ist NICHT Bestandteil dieses Angebots:

- Implementierung von Maßnahmen und Empfehlungen zur Risikominderung
- Sicherheitshärtung, Behebung von Schwachstellen, Patching und Entwicklung von Modulen zur Risikominderung
- Denial-of-Service-Test und -Exploit
- Social Engineering und Client-Side-Angriffe
- sämtliche Tätigkeiten, die nicht ausdrücklich in dieser Dienstleistungsbeschreibung niedergelegt sind

PLANUNG

Die Planungsphase ist entscheidend für den Erfolg des Auftrags. In dieser Phase werden die für die Analyse erforderlichen Informationen zusammengetragen. Dazu zählen Informationen zu u. a. den zu testenden IT-Komponenten, den relevanten Bedrohungen für diese Komponenten sowie den im Analyseansatz zur Risikominderung anzuwendenden Sicherheitskontrollen. Eine Sicherheitsanalyse erfolgt wie jedes andere Projekt auf der Grundlage eines Projektmanagementplans, in dem die Ziele und Ergebnisse, der Leistungsumfang, die Anforderungen, die Rollen und Zuständigkeiten sowie die Grenzen, Erfolgsfaktoren, Annahmen, Ressourcen, zeitliche Planung und Liefergegenstände niedergelegt sind.

Nach dem Projektstart werden die Anforderungen des Kunden erhoben, auf deren Grundlage Ingram Micro einen Entwurf für die Leistungsbeschreibung aufsetzt. Nach Einigung über die Bestimmungen der Leistungsbeschreibung wird der Leistungsumfang umfassend spezifiziert. Dies beinhaltet das Aufsetzen und die Unterzeichnung des Testgenehmigungsschreibens durch beide Parteien sowie eine kurze Besprechung zur Endabstimmung der zeitlichen Planung und Kommunikationsdetails. Das Testgenehmigungsschreiben dient der Bestätigung der Auftragsbedingungen und der Beantwortung aller Fragen vor dem Projektbeginn.

PENETRATIONSTEST FÜR MOBILE ANWENDUNGEN – METHODIK

Der Penetrationstest von Ingram Micro zielt auf die Identifizierung von Schwachstellen, die gemäß Open Web Application Security Project (OWASP) zu den zehn nachstehend aufgeführten wichtigsten Sicherheitsrisiken für mobile Anwendungen zählen.

1. Fehlerhafte Nutzung von Plattformen

Hierunter fallen Fehler bei der Nutzung von Plattformfeatures oder die Nichtnutzung von Sicherheitsprüfungen für Plattformen. Relevant hierbei sind z. B. Android-Intents, Plattformrechte, die unsachgemäße Nutzung von TouchID, der Keychain oder einer anderen Sicherheitskontrolle im Rahmen des mobilen Betriebssystems.

2. Unsichere Datenspeicherung

Schwachstellen im Bereich der Datenspeicherung entstehen, wenn Entwicklerteams annehmen, dass Benutzer oder Malware keinen Zugang zum Dateisystem eines mobilen Endgeräts und damit zu auf dem Gerät gespeicherten sensiblen Daten haben. Dateisysteme sind leicht zugänglich. Unternehmen sollten grundsätzlich davon ausgehen, dass Dateisysteme von Benutzern mit bösen Absichten oder von Malware auf sensible Daten abgesucht werden.

3. Unsichere Kommunikation

Mobile Anwendungen bieten oftmals keinen Schutz für Netzwerk-Traffic. SSL/TLS werden häufig nur zur Authentifizierung genutzt. Diese Inkonsistenz geht mit der Gefahr einher, dass Daten und Sitzungsbezeichner abgefangen werden. Falls doch ein Traffic-Schutz vorhanden ist, sind Fehler bei der Implementierung in der Anwendung möglich. Grundlegende Schwachstellen werden von uns mittels Überwachung des Netzwerk-Traffics des Telefons identifiziert.

4. Unsichere Authentifizierung

Wenn Authentifizierungskonzepte schwach sind oder gar gänzlich fehlen, können Angreifer anonym Funktionen in der mobilen Anwendung im von ihr genutzten Backend-Server ausführen. Ursache für die oftmals schwächere Authentifizierung bei mobilen Anwendungen ist der Input-Formfaktor von Mobiltelefonen.

5. Unzureichende Verschlüsselung

Sind Verschlüsselungsalgorithmen zu schwach oder ist der Verschlüsselungsprozess mangelhaft, können Angreifer verschlüsselten Code oder sensible Daten in ihre ursprüngliche unverschlüsselte Form zurückverwandeln. Auf diese Weise können unbefugt sensible Daten von mobilen Endgeräten abgegriffen werden.

6. Unsichere Autorisierung

Schwächen im Autorisierungskonzept werden identifiziert, indem im Rahmen des Tests Binärangriffe auf die mobilen Anwendungen durchgeführt werden. Ziel dieses Angriffs ist die Ausführung zugangsbeschränkter Funktionen, die nur für Benutzer mit erweiterten Zugangsrechten im „Offline“-Modus ausführbar sein sollten.

7. Qualität des Client-Codes

Diese Art von Schwachstellen ist im Rahmen manueller Code-Überprüfungen nur schwer feststellbar. Stattdessen nutzen Angreifer Drittanbietertools, die statische Analysen oder Fuzzing ermöglichen. Diese Arten von Tools identifizieren Speicherlecks, Pufferüberläufe und andere weniger schwerwiegende Sicherheitslücken, die auf Schwächen bei der Programmierung zurückzuführen sind.

8. Codemanipulation

In der Regel nutzen Angreifer schädliche Formen der App, die in App-Stores Dritter gehostet werden, um Code zu verändern. Auch Phishing-Angriffe sind möglich, bei denen der Benutzer zur Installation der Schad-App verleitet wird. Hierbei relevant sind Binary-Patching, die Veränderung lokaler Ressourcen, Hooking, Swizzling und die dynamische Speicherveränderung.

9. Reverse Engeneering

Mobiler Code ist grundsätzlich anfällig für Zurückentwicklung (Reverse Engineering). Manche Apps sind anfälliger als andere. Code, der in Sprachen oder Frameworks geschrieben ist, die eine dynamische Introspektion zur Laufzeit erlauben (Java, .NET, Objective C, Swift), sind besonders anfällig für Reverse Engineering.

10. Verborgene Funktionen

Manchmal sind verborgene Funktionen sehr wertvoll für Angreifer. Funktionen, die Informationen zu Backend-Tests, Demo-Versionen, Stagings oder UAT-Umgebungen offenlegen, sollten in der Produktivumgebung nicht enthalten sein. Dasselbe gilt für administrative API-Endpunkte oder inoffizielle Endpunkte.

TOOLS

Ingram Micro verwendet sowohl branchenübliche Tools und Frameworks als auch unsere eigenen Skripte. Auf diese Weise gewährleisten wir, dass unsere Penetrationstests möglichst lückenlos und umfassend ist.

Bei unseren Penetrationstests setzen wir u. a. die folgenden Tools ein:

- Burp Suite Pro
- Angr
- Frida
- Ghidra
- Radare2
- MobSF
- Objection
- Apktool
- Drozer
- jadx
- Cycrypt
- Custom Scripts

NACH DER AUSFÜHRUNG

Nach dem Abschluss der Ausführungsphase dokumentiert Ingram Micro alle Erkenntnisse in einem Bericht. Dieser Bericht wird zunächst der internen Qualitätssicherung unterzogen, bevor der Abschlussbericht innerhalb von zwei Wochen nach Auftragsabschluss an den Kunden übermittelt wird.
Dieser Bericht rundet den Auftrag ab und besteht aus einer allgemeinen Zusammenfassung, die als Grundlage für strategische Unternehmensentscheidungen dienen kann, sowie auf einer ausführlichen Analysebeschreibung, anhand derer sich die technischen Aspekte der Tests nachvollziehen lassen.

Der Bericht gliedert sich in die folgenden Abschnitte:

- Allgemeine Zusammenfassung
- Technische Zusammenfassung
- Analysebeschreibung
- Erkenntnisse
- Anhänge (mit Scanergebnissen und Erläuterungen zur Methodik)

ÜBERPRÜFUNG DER ERGRIFFENEN KORREKTURMASSNAHMEN

Falls das Unternehmen die Korrekturmaßnahmen, die zur Behebung der ermittelten Schwachstellen unternommen wurden, überprüfen möchte, führt Ingram Micro diese Überprüfung gerne gegen Aufpreis durch.
Für weitere Informationen und die zeitliche Planung steht Ihnen Ihr Channel-Partner gerne zur Verfügung.

PFLICHTEN DES KUNDEN

Der Kunde verpflichtet sich zur Erfüllung seiner Pflichten und erkennt an und erklärt sich damit einverstanden, dass **die Erfüllung der Pflichten von Ingram Micro von dem Folgenden abhängt:**

- Die Ressourcen des Kunden stehen Ingram Micro plangemäß zur Verfügung.
- Alle zu analysierenden Server und Netzwerke sind bei Durchführung der Analyse in Betrieb und funktionsfähig.
- Der Kunde stellt sämtliche angefragten Dokumente und Informationen rechtzeitig und im Einklang mit den in der Planungsphase festgelegten Lieferterminen zur Verfügung.
- Zu Testzwecken wird jede im Leistungsumfang enthaltene IP als separater Host betrachtet, und zwar unabhängig vom potenziellen Lastenausgleich, von Firewalls usw.
- Sofern keine anderweitigen Bedingungen mit dem Unternehmen vereinbart wurden, werden sämtliche Test- und Analysetätigkeiten in einem Zeitfenster von 24 Stunden durchgeführt.
- Die Testzeitfenster des Kunden müssen lange genug für die Durchführung der Tätigkeiten sein.

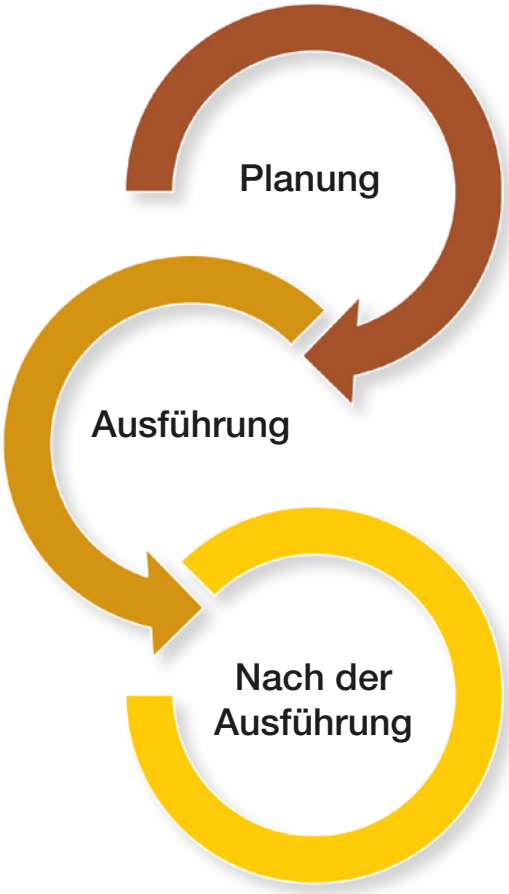
Es gelten die vor Ort anwendbaren Allgemeine Geschäftsbedingungen von Ingram Micro.

Penetrationstest für Cloud Umgebungen

Der Penetrationstest für Cloud Umgebungen zielt auf Schwachstellen in Design, Deployment und Konfiguration von Umgebungen, die in der Cloud gehostet werden. Dabei macht Ingram Micro Gebrauch von zahlreichen Tools, Techniken und Verfahren, mittels derer die Sicherheit im Unternehmen von sowohl extern als auch intern beleuchtet wird. Angreifer machen sich häufig Fehlkonfigurationen und mangelhafte Zugangskonzepte zunutze. Wir klären unsere Kunden über die Risiken auf und schlagen Maßnahmen zu Verbesserung der Sicherheit und Compliance der Kundenumgebung vor.

Unsere Methodik gründet u.a. auf den folgenden Branchenstandards:

- Penetration Testing Execution Standard (PTES)
- NIST 800-115
- Open-Source Security Testing Methodology Manual (OSSTMM)
- MITRE ATT&CK
- Cloud Security Alliance (CSA) Cloud Penetration Testing Playbook



- Sammeln von Informationen zwecks Festlegung des Leistungsumfangs
- Bestätigung der Leistungsbeschreibung
- Aufsetzen des Testgenehmigungsschreibens

- Reconnaissance
- Bedrohungsmodellierung
- Schwachstellenanalyse
- Exploitation
- Post-Exploitation

- Erstellung des Berichts
- Qualitätssicherung
- Präsentation

LEISTUNGSUMFANG

Mit dem Penetrationstest für Cloud Umgebungen möchte Ingram Micro unseren Kunden dabei helfen, Sicherheitslücken zu schließen, indem Schwachstellen im gesamten Deployment identifiziert werden. Bei der Bewertung der Infrastruktur kommen sowohl automatisierte als auch manuelle Methoden zum Einsatz.

Das Angebot umfasst die folgenden Prozesse, die entweder einzeln oder in Kombination umgesetzt werden:

- **Externer Cloud-Test**
  Dieser Test erfolgt aus der Perspektive eines Angreifers, der vom öffentlichen Raum aus angreift und nicht über Vorkenntnisse zu den genutzten Systemen und Technologien verfügt. Mit diesem sogenannten „Black-Box-Test“ werden die öffentlichen Angriffsflächen, über die Daten leicht zugänglich sind und missbraucht werden können, realistisch nachgezeichnet. Zusätzlich werden Scans und manuelle Tests durchgeführt, um vorhandene Schwachstellen aufzuzeigen.
- **Interner Cloud-Test**
  Ausgehend von der Annahme, dass das Unternehmensnetzwerk bereits Ziel eines Angriffs geworden ist („Assumed Compromise“), werden die Netzwerkschichten und virtuellen Maschinen des Unternehmens getestet. Dabei wird ein Angriff simuliert, bei dem sich der Angreifer bereits in der Umgebung des Unternehmens befindet.
- **Konfigurationsprüfung**
  Ingram Micro analysieren die genutzten Dienste und ihre Konfigurationen. Das Identitäts- und Zugangsmanagement (IAM) spielt eine wichtige Rolle bei der Senkung des Angriffsrisikos.

GRENZEN DES LEISTUNGSUMFANGS

Das Folgende ist NICHT Bestandteil dieses Angebots:

- Implementierung von Maßnahmen und Empfehlungen zur Risikominderung
- Sicherheitshärtung, Behebung von Schwachstellen, Patching und Entwicklung von Modulen zur Risikominderung
- Denial-of-Service-Test und -Exploit
- Social Engineering und Client-Side-Angriffe
- sämtliche Tätigkeiten, die nicht ausdrücklich in dieser Dienstleistungsbeschreibung niedergelegt sind

PLANUNG

Die Planungsphase ist entscheidend für den Erfolg des Auftrags. In dieser Phase werden die für die Analyse erforderlichen Informationen zusammengetragen. Dazu zählen Informationen zu u. a. den zu testenden IT-Komponenten, den relevanten Bedrohungen für diese Komponenten sowie den im Analyseansatz zur Risikominderung anzuwendenden Sicherheitskontrollen. Eine Sicherheitsanalyse erfolgt wie jedes andere Projekt auf der Grundlage eines Projektmanagementplans, in dem die Ziele und Ergebnisse, der Leistungsumfang, die Anforderungen, die Rollen und Zuständigkeiten sowie die Grenzen, Erfolgsfaktoren, Annahmen, Ressourcen, zeitliche Planung und Liefergegenstände niedergelegt sind.

Nach dem Projektstart werden die Anforderungen des Kunden erhoben, auf deren Grundlage Ingram Micro einen Entwurf für die Leistungsbeschreibung aufsetzt. Nach Einigung über die Bestimmungen der Leistungsbeschreibung wird der Leistungsumfang umfassend spezifiziert. Dies beinhaltet das Aufsetzen und die Unterzeichnung des Testgenehmigungsschreibens durch beide Parteien sowie eine kurze Besprechung zur Endabstimmung der zeitlichen Planung und Kommunikationsdetails. Das Testgenehmigungsschreiben dient der Bestätigung der Auftragsbedingungen und der Beantwortung aller Fragen vor dem Projektbeginn.

PENETRATIONSTEST FÜR CLOUD ANWENDUNGEN – METHODIK

Die Penetrationstests von Ingram Micro basieren auf bewährten Verfahren und den besten Angriffsmethoden und liefern eine lückenlose, umfassende Analyse zur Cloud-Sicherheit. Dabei wird mittels verschiedener Methoden fehlkonfigurierte Speicherdienste identifiziert, darunter AWS-S3-Buckets oder Azure Storage Blobs, Enumeration von Azure-Active-Directory-Einheiten, Eskalation der Zugangsrechte mit Azure Runbooks sowie Automation-Konten, Datenexfiltration und Mining.

Reconnaissance

- Suche nach manipulierbaren öffentlich verfügbaren Informationen
- Suche nach frei zugänglichen Zugangsschlüsseln in GitHub-Speichern
- Identifizierung fehlkonfigurierter Speicherdienste

Discovery

- Port-Scan
- System-Fingerprinting
- Enumeration

Schwachstellenanalyse

- Vorbereitung der Exploitation

Exploitation

- Manuelle Schwachstellenprüfung und Verifizierung identifizierter Schwachstellen
- Prüfung von Firewalls und Intrusion-Detection- bzw. -Prevention-Systemen
- Passwort-Spraying mit gängigen und schwachen Passwörtern

Post-Exploitation

- Enumeration im lokalen System
- Enumeration im Netzwerk und Pivoting
- Identifizierung sensibler Daten
- Exfiltration

TOOLS

Ingram Micro verwendet sowohl branchenübliche Tools und Frameworks als auch unsere eigenen Skripte. Auf diese Weise gewährleisten wir, dass unsere Penetrationstests möglichst lückenlos und umfassend sind.

Bei unseren Penetrationstests setzen wir u. a. die folgenden Tools ein:

- Pacu
- ScoutSuite
- Buckethead
- Trufflehog
- Gitleaks
- AzureHound
- AADInternals
- MicroBurst
- ROADTools
- Nmap
- Nessus Professional
- Burp Suite Pro
- Metasploit Framework
- Custom Scripts

NACH DER AUSFÜHRUNG

Nach dem Abschluss der Ausführungsphase dokumentiert Ingram Micro alle Erkenntnisse in einem Bericht. Dieser Bericht wird zunächst der internen Qualitätssicherung unterzogen, bevor der Abschlussbericht innerhalb von zwei Wochen nach Auftragsabschluss an den Kunden übermittelt wird.
Dieser Bericht rundet den Auftrag ab und besteht aus einer allgemeinen Zusammenfassung, die als Grundlage für strategische Unternehmensentscheidungen dienen kann, sowie auf einer ausführlichen Analysebeschreibung, anhand derer sich die technischen Aspekte der Tests nachvollziehen lassen.

Der Bericht gliedert sich in die folgenden Abschnitte:

- Allgemeine Zusammenfassung
- Technische Zusammenfassung
- Analysebeschreibung
- Erkenntnisse
- Anhänge (mit Scanergebnissen und Erläuterungen zur Methodik)

ÜBERPRÜFUNG DER ERGRIFFENEN KORREKTURMASSNAHMEN

Falls das Unternehmen die Korrekturmaßnahmen, die zur Behebung der ermittelten Schwachstellen unternommen wurden, überprüfen möchte, führt Ingram Micro diese Überprüfung gerne gegen Aufpreis durch.
Für weitere Informationen und die zeitliche Planung steht Ihnen Ihr Channel-Partner gerne zur Verfügung.

PFLICHTEN DES KUNDEN

Der Kunde verpflichtet sich zur Erfüllung seiner Pflichten und erkennt an und erklärt sich damit einverstanden, dass **die Erfüllung der Pflichten von Ingram Micro von dem Folgenden abhängt:**

- Die Ressourcen des Kunden stehen Ingram Micro plangemäß zur Verfügung.
- Alle zu analysierenden Server und Netzwerke sind bei Durchführung der Analyse in Betrieb und funktionsfähig.
- Der Kunde stellt sämtliche angefragten Dokumente und Informationen rechtzeitig und im Einklang mit den in der Planungsphase festgelegten Lieferterminen zur Verfügung.
- Zu Testzwecken wird jede im Leistungsumfang enthaltene IP als separater Host betrachtet, und zwar unabhängig vom potenziellen Lastenausgleich, von Firewalls usw.
- Sofern keine anderweitigen Bedingungen mit dem Unternehmen vereinbart wurden, werden sämtliche Test- und Analysetätigkeiten in einem Zeitfenster von 24 Stunden durchgeführt.
- Die Testzeitfenster des Kunden müssen lange genug für die Durchführung der Tätigkeiten sein.

Es gelten die vor Ort anwendbaren Allgemeine Geschäftsbedingungen von Ingram Micro.

ANSPRECHPARTNER

Christian Voss-Freund
System Engineer
Tel. +49.89.4208.2629
christian.voss-freund@ingrammicro.com

Cyber Security Business Unit
cybersecurity@ingrammicro.de

INGRAM MICRO®
SECURITY

INGRAM MICRO B.V. – PAPENDORPSEWEG 95 – 3528 BJ UTRECHT – NIEDERLANDE