Security Testing Services

claranet cyber security®

Das Portfolio


Infrastructure


Web Apps


Mobile Apps


Red Team


Phishing & Smishing


Firewall Review


Mobile Devices (onsite)


Physical Security (onsite)


Cloud


Social Engineering


Code Review


WiFi (onsite)


Desktop Breakout


Intelligence Gathering


Container & Kubernetes


M365 Health Check

claranet cyber security®

Web Application Testing

Webanwendungen sind für Hacker rund um die Uhr zugänglich und stecken voller Daten – ein verlockendes Ziel. Unsere Penetrationstests beruhen auf der manuellen Ausnutzung von Schwachstellen, so dass Sie die Einschätzung des Geschäftsrisikos erhalten, die nur ein Experte liefern kann. Wir kombinieren dies mit dem Einsatz der besten automatisierten Tools. Im Anschluss an alle Bewertungen erstellen wir einen umfassenden Bericht, der sowohl nichttechnische als auch technische Beschreibungen sowie Empfehlungen für Abhilfemaßnahmen enthält.

Wir machen Risiken sichtbar, darunter:

- Unbefugter Zugriff unter Umgehung der Authentifizierungskontrollen zur Ausweitung von Privilegien
- Einschleusen von bösartigem Code
- Manipulation der Funktion der Anwendung
- Verunstaltung der Website oder Verursachen von Unterbrechungen
- Erlangung von Zugang zur Hosting-Infrastruktur

Zusätzlich zu unseren punktuellen Webanwendungstests bieten wir auch kontinuierliche Sicherheitstests und Security Operations Center (SOC)-Dienste an, damit Sie rund um die Uhr geschützt sind. Bitte fragen Sie uns nach Details.

claranet cyber security®

Mobile Application Testing

Mit der enormen Verbreitung mobiler Anwendungen steigt auch der Bedarf an anspruchsvollen Sicherheitstests, mit denen überprüft werden kann, ob mobile Anwendungen Systeme und Daten in gleichem Maße schützen wie Standard-Webanwendungen.

Ziel der Übung ist es, zu überprüfen, ob die mobile Anwendung sicher kodiert ist und Angreifer daran gehindert werden, Authentifizierungskontrollen zu unterlaufen, Privilegien zu erweitern, bösartigen Code einzuführen oder die Funktionalität der Anwendung zu manipulieren, um ihre Ziele zu erreichen. Jedes Versäumnis, sensible Informationen korrekt zu maskieren und/oder zu speichern, könnte zu einem Durchsickern von Informationen und ihrer Verwendung durch andere als die vorgesehenen Anwendungen führen.

Die Prüfung mobiler Anwendungen validiert:

- die Verschlüsselung von Daten sowohl bei der Übertragung als auch im Ruhezustand
- Webdienste
- Offenlegung von Informationen durch lokale Datenspeicherung
- APIs zwischengespeicherte Daten wie z. B. Anwendungshintergründe

claranet cyber security®

Infrastruktur Testing

Das Hauptziel von Infrastrukturtests besteht darin, Schwachstellen in Computersystemen aufzuzeigen, die einen unbefugten Zugang zu privaten Bereichen des Netzes oder zu sensiblen Daten ermöglichen könnten.

Infrastrukturtests können in vielen Bereichen durchgeführt werden, darunter intern, am Netzwerkrand und in der Cloud. Sie gilt auch für viele Technologiebereiche, von PCs und Laptops bis hin zu Smartphones und Wi-Fi-Netzwerken. Aus der Sicht eines Hackers stellt jeder Bereich eine Angriffsmöglichkeit dar, die durch eine Überprüfung Ihrer Sicherheit auf die gleiche Weise wie bei Ihren Gebäuden oder physischen Anlagen minimiert werden kann.

Um einen ausführlichen Überblick über die Schwachstellen und die damit verbundenen Ausnutzungsmöglichkeiten zu erhalten, können Infrastrukturtests als eigenständige Übung oder als Element eines umfassender simulierten Angriffs eingesetzt werden.

Social Engineering Assessments

Social Engineering wird zu einem der effektivsten Mittel, um sich Zugang zu sicheren Systemen und sensiblen Informationen zu verschaffen. Darüber hinaus benötigt der Angreifer wenig bis gar keine technischen Kenntnisse. Die Verhinderung eines solchen Angriffs erfordert ein ganz anderes Abwehrsystem als das herkömmliche der Cybersicherheit.

Sensibilisierung der Mitarbeiter

Die beste Verteidigungsstrategie gegen Social Engineering besteht darin, das Bewusstsein der Mitarbeiter zu schärfen und sie über gute Praktiken aufzuklären. Mit einer Social-Engineering-Bewertung von Claranet Cyber Security können Sie feststellen, wie anfällig Ihre Mitarbeiter sind, wenn ein Angreifer versucht, sie auszutricksen. Die Ergebnisse dieser Bewertungen können für Schulungen, die Erstellung von Richtlinien für den Umgang mit Daten und Sicherheitsrichtlinien verwendet werden.

Typische Social-Engineering-Einsätze sind:

- Phishing- und Spear-Phishing-Kampagnen: Täuschung von Benutzern per E-Mail
- Physisches Eindringen: Erlangung von unbefugtem Zugang zu Gebäuden
- Köder: Verleiten von Benutzern zum Einstecken von USB-Laufwerken
- Identitätswechsel von Mitarbeitern: um Informationen oder Zugang aus der Ferne zu erhalten

claranet cyber security®

Red Teaming

Eine Red-Team-Übung ist ein umfassender Versuch, die festgelegten Ziele mit allen verfügbaren Methoden zu erreichen, und umfasst in der Regel interne und externe Penetrationstests, die Kompromittierung drahtloser Netzwerke, physischen Zugang und andere Social-Engineering-Techniken.

Red-Team-Übungen werden nach einem Black-Box-Testing-Ansatz durchgeführt, bei dem keine Vorabinformationen über die Zielorganisation vorliegen. Während eines Red-Team-Einsatzes weiß die verteidigende Seite nichts von der Übung und es wird erwartet, dass sie wie bei einem echten Angriff reagiert.

Gemeinsame Ziele von Red Teams:

- **Foothold**: Standardbenutzerzugang (Shell/GUI) von außen
- **Privilege Escalation**: Erlangung administrativer Benutzerprivilegien
- **Defence Evasion**: Umgehen von externen/internen Sicherheitswarnsystemen
- **Persistence**: Der Fernzugriff ist nicht von einem einzigen Benutzerkonto oder einem einzigen Gerät abhängig
- **Lateral Movement**: Traversal zu mehreren Punkten in einem Netzwerk
- **Full Compromise**: Domänen-/Enterprise-Admin-Konto oder gleichwertiges Konto kompromittiert
- **Collection**: Aktion auf Ziele
- **Exfiltration**: Exfiltration von Daten

claranet cyber security®

Security Checks

Neben unseren Pentests bieten wir detaillierte Security Checks für verschiedenste Ziele an. Hierbei prüfen wir das Ziel sowhl auf offene Schwachstellen als auch Fehlkonfigurationen. Folgendes können wir zeitnah und zuverlässig für Sie prüfen:

- **Firewall inkl. des Regelwerkes für alle Hersteller**
- **Azure Cloud**
- **AWS Cloud**
- **Google Cloud**
- **Container-Umgebung**
- **Kubernetes-Setup**
- **SAP-System**

claranet cyber security®

Warum Claranet?

Schnelle Lieferfähigkeit mit über 70 Pentestern weltweit

Nur maßgeschneidertes, manuelles Penetration Testing

+10.000 Tage pro Jahr Penetration Testing bei unseren Kunden

Internes Pentesting-Team mit hohem Skill-Level

Über 25 Jahre Erfahrung

claranet cyber security®

Über Claranet

Quick Facts

- 1996 gegründet
- Inhabergeführt
- € 600 Mio jährlicher Umsatz
- Globale Reichweite mit Niederlassungen in 11 Ländern
- Über 10.000 Geschäftskunden
- Mehr als 3.500 Mitarbeitende in 24 Büros
- Langfristige Kundenbeziehungen

claranet cyber security®


claranet
cyber
security®

Weitere Informationen über **Security Testing Services:**

+49 (0)69 40 80 18 450

claranet cyber security®