Cyber Security Offensive

ConSecur

[security and consulting]

Angriff ist die beste Verteidigung

Stellen Sie sich Ihre IT als Festung vor: hochgezogen mit Firewalls, Zugangskontrollen und Überwachungssystemen. Für fast alle IT-Verantwortlichen stellt sich die Gretchenfrage: Wie stabil sind diese Mauern wirklich? Die Antwort finden wir auf, indem wir den Ernstfall simulieren.

VERSCHAFFEN SIE SICH KLARHEIT:

In Ihrem Auftrag greifen wir diese Festung an. Unser Offensive Cyber Security Team agiert wie ein echter Angreifer – raffiniert, kontrolliert, hartnäckig und im Dienst Ihrer Sicherheit.

So werden Sicherheitslücken sichtbar, bevor Cyber-Kriminelle sie ausnutzen. Verteidigung stärken ConSecur Offensive Cyber Security Services geben IT-Verantwortlichen die Grundlage, ihre Verteidigung gezielt zu verstärken.

Problemstellung Verteidigungsfähigkeit testen: Best Practice vs. Red Teaming

Viele Sicherheitsprodukte und Beratungen setzen auf Best-Practice-Lösungen. Diese sind hilfreich – aber sie reichen oft nur, um einfache Angriffe wie Commodity-Malware oder unerfahrene Pentester zu detektieren.

DAS PROBLEM:

Reale Angreifer und Red Teamer gehen anders vor: Sie denken unkonventionell, sie sind hartnäckig und nutzen auch menschliche Schwachstellen. Genau deshalb finden sie Lücken, die zuvor niemand gesehen hat – und die in Standard-Tests unentdeckt bleiben.

UNSER ANSATZ GEHT EINEN SCHRITT WEITER:

Wir simulieren realistische Angriffe mit der Finesse und Kreativität echter Angreifer. So werden genau die Schwachstellen sichtbar, die Standard-Methoden übersehen – und Ihre Sicherheitsarchitektur erhält den Härtetest, den sie wirklich braucht.

ANGRIFF:

Für Ihre Sicherheit wechseln wir die Seiten

01

SCHWACHSTELLEN MANAGEMENT SCHWACHSTELLENANALYSE

Sicherheitslücken erkennen und priorisieren.

02

PHYSISCHER SICHERHEITSCHECK SOCIAL ENGINEERING

Zugangskontrolle und Sicherheitsmechanismen vor Ort im Blick.

03

TECHNISCHER PENTEST (INTERN/ EXTERN)

Gezielte Sicherheitstests auf Ihre IT-Infrastruktur durch kontrollierte Angriffe.

04

TECHNISCHER PENTEST (WEBANWENDUNG/WEBSERVICE)

Sicherheitslücken in Webanwendungen/Webservices systematisch aufdecken. Simulierter Cyberangriff.

05

RED TEAMING

Praxisnahe Angriffssimulation zur Messung Ihres tatsächlichen Sicherheitsniveaus- über Technik, Prozesse und Menschen hinweg.

06

PHISHING

Simulation realistischer Phishing-
Angriffe zur Bewertung der Wirksamkeit von technischen Sicherheitsmechanismen und der Sensibilisierung Ihrer Mitarbeitenden.

Deshalb ConSecur

Cyber-Kriminelle arbeiten hochprofessionell, organisiert und mit erstaunlicher Kreativität. Sie suchen die versteckten Wege, die niemand auf dem Zettel hat.

DIESE REALITÄT ERLEBEN WIR TÄGLICH.
In unserem Cyber Defense Center analysieren wir kontinuierlich echte Angriffe. Wir sind konfrontiert mit Phishing-Kampagnen, Ransomware und mit gezielten Attacken auf kritische Infrastrukturen. Wir sehen, wie Angreifer vorgehen.

Wir erleben, welche neuen Taktiken sie entwickeln und wo Verteidigungsmechanismen versagen. Dieses Wissen ist kein Lehrbuchwissen, sondern unmittelbare Praxiserfahrung.

FÜR IHRE SICHERHEIT WECHSELN WIR DIE SEITEN:

Wir greifen Ihre IT-Infrastruktur an!

Hält Ihre IT einem realistischen Angriff stand?

Welche neuen Wege haben wir gefunden, Ihre Sicherheitsvorkehrungen zu umgehen?

Die Auswertung zeigt, wie erfolgreich unsere simulierte Cyber-Attacke auf Ihre IT-Infrastruktur gewesen ist.

WISSEN AUS PRAXIS UND THEORIE SIND DIE BASIS UNSERER OFFENSIVE SECURITY SERVICES.

PROFITIEREN SIE VON:

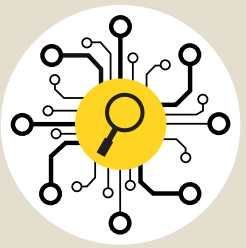
- jahrzehntelanger Erfahrung im Security Consulting – wir kennen Theorie und Praxis
- maßgeschneiderten Modulen, die individuell für Ihre Umgebung kombiniert werden.
- eigenen Tools, die reale Angriffe abbilden, statt Standardschemata abzuprüfen.
- SOC- und Incident-Response-Kompetenz, die uns erlaubt, auch Detection & Response Ihrer Systeme mit einzubeziehen.
- kontinuierlicher Weiterentwicklung, weil Angreifer nie stillstehen – und wir auch nicht.

Das Ergebnis ist eine realistische Einschätzung der Sicherheit Ihrer IT-Infrastruktur.

Zu Ihrer Sicherheit:
Wir wechseln die Seiten und greifen Ihre IT-Infrastruktur an.

ANGRIFFSSIMULATION IN 4 SCHRITTEN

So greifen wir Ihre IT-Infrastruktur an



BEDARFSERMITTLUNG

WOMIT STARTEN WIR?
Gemeinsam prüfen wir, mit welcher Methode wir Ihre IT-Infrastruktur angreifen werden. Penetration Test, RedTeaming oder etwas anderes: Womit identifizieren wir die Schwachstellen in Ihrer IT-Infrastruktur?

PLANUNG

WIE GEHEN WIR VOR?
Gemeinsam definieren wir Ziele und Umfang, legen Erfolgskriterien fest und stecken Rahmenbedingungen ab. Dahinter verbergen sich Kommunikationswege und Informationen, die wir für eine gute Vorbereitung kennen möchten.

UMSETZUNG

WO SIND DIE LÜCKEN?
Wir haben die Seiten gewechselt und greifen an. Unsere Aufgabe ist, Ihre IT-Infrastruktur zu attackieren, zu kompromittieren, anzugreifen. Wir nehmen die Technik ins Visier und den Menschen. Wir wollen Ihre Festung stürmen!

AUSWERTUNG & ABSCHLUSS

WAS TUN SIE ALS NÄCHSTES?
Das Ergebnis liegt vor: Nach dem simulierten Angriff wissen wir, ob Ihre IT-Infrastruktur Schwachstellen aufweist und welche das sind. Anhand der vorliegenden Dokumentation besprechen wir die nächsten Schritte, die wir Ihnen als konkrete Handlungsempfehlungen vorstellen.

ConSecur GmbH

Als herstellerunabhängiges Beratungs- und Dienstleistungsunternehmen befasst sich die ConSecur GmbH mit der Planung und Umsetzung von Maßnahmen zur Informationssicherheit. Unsere Leidenschaft ist die Entwicklung, Bewertung und Realisierung von IT-Sicherheitskonzepten für Unternehmen. So beschützen wir die Information, die Sie täglich für Einkauf, Produktion, Dienstleistung, Logistik und Korrespondenz benötigen. ConSecur hat sich darauf spezialisiert Informationssicherheit an die Geschäftsprozesse im organisatorischen und informationstechnischen Umfeld anzubinden. Hierbei setzen wir auf die bestehenden unternehmerischen Prozesse und eingesetzten Technologien unserer Kunden auf. Wir etablieren lösungsorientierte, standardisierte und effiziente Maßnahmen, die unsere Kunden in die Lage versetzen, ihre informationstechnischen Risiken zu beherrschen und bestehenden regulatorischen Vorgaben zu genügen. Ziel unserer Arbeit ist es, nur berechtigten Personen den Zugriff auf Informationen zu gewähren und Informationen vor Übergriffen Unbefugter zu schützen

ConSecur – next level information security

ConSecur
[security and consulting]

ConSecur GmbH
Nödiker Straße 118
49716 Meppen

TEL.: +49 5931 9224-0
info@ConSecur.de
www.ConSecur.de