CYBERSEC-NG
Swiss Cybersecurity

Penetration Tests & Vulnerability Assessments

KONTINUIERLICHE IT-SICHERHEIT

Im Jahr 2020 wurden in einer der bekanntesten Schwachstellen-datenbanken der Welt (CVE-Details) um die 17‘000 Schwachstellen gemeldet. Im Schnitt werden also monatlich ca. 1’400 neue Schwachstellen entdeckt. Daraus ergibt sich, dass eine kontinuerliche Überprüfung Ihrer IT-Infrastruktur und Applikationen unabdingbar geworden ist.

WEBSEITENSCHUTZ

Web Applikationen werden durch den Einsatz moderner Technologien zunehmend komplexer. Komplexität führt zu einer grösseren Angriffsfläche und entsprechend zu mehr Schwachstellen. Häufig werden kritische, verwundbare Web Applikationen in der Praxis durch eine Web Application Firewall (WAF) geschützt. Problematisch bei diesem Ansatz ist, dass die WAF einen «Single Point of Failure» darstellt. Miskonfigurationen oder gar der Ausfall einer WAF führt dazu, dass die Web Applikation exponiert und angreifbar wird. Unsere Dienstleistungen helfen Ihnen Schwachstellen in Ihren Web Applikationen aufzufinden, diese zu härten und die Abhängigkeit von WAF’s zu reduzieren.

Penetration Tests und Vulnerability Assessments haben das Ziel IT-Sicherheitsschwachstellen in Systemen und/oder Applikationen sichtbar zu machen, damit diese proaktiv behoben werden können. Häufig werden Penetration Tests und Vulnerability Assessments in der Praxis verwechselt oder als einheitlicher Begriff verwendet obwohl markante Unterschiede bestehen. Wann sollte also ein Penetration Test und wann ein Vulnerability Assessment durchgeführt werden?

Vulnerability Assessment

Das Ziel bei der Durchführung eines Vulnerability Assessments ist die Auffindung möglichst vieler IT-Sicherheitsschwachstellen innerhalb eines gegebenen Zeitraums. Bei diesem Ansatz geht es also darum, eine möglichst breite Abdeckung bei der Auffindung von IT-Sicherheitsschwachstellen, auf Kosten der Tiefe, zu erreichen. Die gefundenen Schwachstellen werden verifiziert aber nicht nicht ausgenutzt (Exploiting).

Zusammengefasst ergeben sich die folgenden Vorteile bei einem Vulnerability Assessment:

- Breite Abdeckung bei der Auffindung von IT-Sicherheitsschwachstellen.
- Identifikation, Analyse und Risk Assessment der gefundenen IT-Sicherheitsschwachstellen.
- Reduziert die Wahrscheinlichkeit auf einen erfolgreichen Cyberangriff erheblich.
- Ermöglicht es eine Übersicht über den technischen Sicherheitszustand Ihrer Applikationen und/oder Systeme zu erhalten. Dies ist insbesondere Wertvoll, falls noch nie ein Vulnerability Assessment durchgeführt wurde.
- Dient als Basis für künftige IT-Security Massnahmen, die zielgesetzter angewendet werden können.

Penetration Tests

Das Ziel bei der Durchführung eines Penetration Tests ist häufig die Simulation von realen Cyberangriffen oder das Überwinden von spezifischen Sicherheitsmechanismen. Bei diesem Ansatz geht es also darum, Schwachstellen in der Tiefe aber nicht in der Breite ausfindig zu machen und diese soweit wie möglich auszunutzen. Entsprechend lohnt sich die Durchführung eines Penetration Tests zur Überprüfung von gut gesicherten Systemen und/oder Applikationen.

Zusammengefasst ergeben sich die folgenden Vorteile bei einem Penetration Test:

- Spezifische, tiefgehende Suche nach IT-Sicherheitsschwachstellen.
- Durchführung von authorisierten, realen Cyberangriffen.
- Überprüfung von internen IT-Sicherheitsprozessen und der User Awareness.
- Ausnutzung von Sicherheitsschwachstellen

CYBERSEC-NG
Swiss Cybersecurity

NETZWERKSCHUTZ

Unser Dienstleistungen ermöglichen es Ihnen Schwachstellen in Ihrem Perimeter zu erkennen und zu beheben bevor diese von Cyberkriminellen ausgenutzt werden.

IT RISK MANAGEMENT

Sie erkennen aktuelle technische Sicherheitsrisiken, die Ihre IT-Infrastruktur und Applikationen bedrohen und sind in der Lage diese proaktiv zu beheben.

AWARENESS

Durch gezielte, realistische Cyberangriffe können Sie Ihre internen Sicherheitsprozesse überprüfen und trainieren. Zudem erhöht sich bei regelmässiger Durchführung auch die User Awareness.

Dienstleistungen

Wir lehnen uns bei der Durchführung von Penetration Tests und Vulnerability Assessments an die gängigen Industriestandards wie OWASP, PTES und OSSTMM. Die folgende Grafik zeigt eine Übersicht der am häufigsten nachgefragten Dienstleistungen im Bezug auf Penetration Testing und Vulnerability Assessments. Auf Anfrage behandeln wir auch gerne weitere Themen.

Web Applications

Web Applikationen finden eine breite Anwendung und sind aus unserem Alltag kaum noch wegzudenken. Sei es beim Online-Shopping, E-Banking, Streaming, der Steuererklärung oder der Bestellung eines Zugtickets, fast alles kann über das Internet respektive Web Applikationen abgewickelt werden.

Dieses Potential haben natürlich auch Cyberkriminelle erkannt und führen verschiedene Cyberangriffe auf Web Applikationen durch. Ihr Ziel ist meist monetärer Gewinn, politischer Aktivismus, Diffamierung oder auch die Ausschaltung der Konkurrenz (Betriebsspionage, Denial of Service). Der daraus entstehende Schaden hat sich in der Vergangenheit in Form von Datenleaks, Distributed Denial of Service (DDoS) Angriffen, Server Übernahmen, Defacements und vielem mehr gezeigt. Fast täglich finden sich in den Medien Schlagzeilen über diese und ähnliche Cyberangriffe, was zu einem weltweit geschätzen Schaden von ca. 600 Milliarden Franken (2019) geführt hat.

Wir helfen Ihnen Ihre Web Applikationen abzusichern indem wir IT-Sicherheitsschwachstellen ausfindig machen und Ihnen zeigen, wie Sie diese beheben können.

Web Services

Durch die laufenden Weiterentwicklungen und Innovationen im Bereich von Web Applikationen haben sich die Web Services herausgebildet. Web Services dienen häufig als Schnittstelle zwischen Systemen und/oder Applikationen. Eines der wahrscheinlich häufigsten Einsatzgebiete besteht im Zusammenhang mit Mobile Applikationen (Android / iOS). Der Webservice übernimmt hierbei die Schnittstelle zwischen der Mobile Applikation (auf dem Smartphone installierte App) und dem Backend.

Es zeigen sich ähnliche Angriffsvektoren (Denial of Service, Server Übernahmen, Datenleaks, etc.) wie bei den oben erwähnten Web Applikationen. Insbesondere gegenüber dem Internet exponierte Webservices stellen ein beliebtes Angriffsziel für Cyberkriminelle dar.

CYBERSEC-NG
Swiss Cybersecurity

KONTAKT
Cybersec-ng GmbH
Grünaustrasse 1
3084 Wabern
office@cybersec-ng.ch
078 729 38 39

Mobile Applications

Mit der Einführung des Smartphones hat eine wahrhafte Explosion in der Zunahme von Mobile Applikationen stattgefunden. Aktuell sind Millionen von Mobile Applikationen in den verschiedenen Appstores von Google und Apple verfügbar.

Mobile Applikationen oder sogenannte «Apps» bestehen häufig aus einer clientseitigen Komponente (die installierte App) und einer serverseitigen Komponente (Web Service), die die Anfragen des Benutzers entgegennimmt und an das Backend weiterleitet. Dadurch entstehen zwei potentielle Angriffsziele für Cyberkriminelle. Wir empfehlen bei der Durchführung von Mobile Application Penetration Tests oder Vulnerability Assessments grundsätzlich die Analyse aller involvierter Komponenten.

Internet of Things (IoT)

Unter dem Internet of Things handelt es sich gnerell um kostengünstige, mit dem Internet verbundene Geräte, die Daten mit anderen Geräten und Systemen austauschen. Im privaten Bereich finden sich IoT Geräte in Form von Produkten wie Alexa, Google Home, Smart Homes oder Webcams. Im geschäftlichen Umfeld werden IoT Geräfe häufig für den Austausch von Sensordaten bei der industriellen Produktion (Smart Manufacturing), Strom (Smart Grid) oder auch im medizinischen Bereich eingesetzt.

Problematisch bei IoT Geräten ist der häufig schlechte Zustand der IT-Security. Dieses Problem hat sich deutlich bei einem der grössten Botnetze der Welt (Mirai) gezeigt, das ausschliesslich aus schlecht abgesicherten IoT Geräten bestand und für Distributed Denial of Service Attacken verwendet wurde. Die mangelnde IT-Security bei IoT Geräten kann auch dazu führen, dass die Kontrolle über Ihr Smart Home übernommen wird, ihr Kühlschrank Spam Mails versendet, Teil eines Botnets zur Durchführung von Distributed Denial of Service oder weiteren Cyberangriffen wird.

Externe / Interne Netzwerke

Einer der ersten Schritte bei einem gezielten Cyberangriff auf Ihr Unternehmen ist die sogenannte Recon-Phase. In dieser Phase scannt der Angreifer Ihre extern verfügbaren, gegenüber dem Internet exponierten Netzwerkservices (Web Applikationen, SSH, FTP, etc.) und sucht nach IT-Sicherheitsschwachstellen. Durch neue Services wie Shodan, kann die Recon Phase auch ohne direkte Scans durchgeführt werden. Falls der Angreifer eine kritische Schwachstelle im Perimeter findet, kann ihm unter anderem der Zugang zum internen Firmennetzwerk gelingen, wo er sich weiter ausbreiten kann.

Zum Schutz von externen Netzwerken bieten sich unser Vulnerability Scanning Service an (siehe Factsheet). Durch den von uns entwickelten Multivendor Schwachstellenscanner können Sie einmalig oder periodisch Ihren Perimeter automatisiert auf aktuelle IT-Sicherheitsschwachstellen überprüfen und diese beheben.

Auch die Sicherheit der internen IT-Netzwerke sollte nicht vernachlässigt werden. In der Praxis wird der externe Perimeter relativ gut geschützt, während sich die Sicherheit des internen Netzwerks in einem schlechten Zustand befindet. Sollte also ein Angreifer den externen Perimeter beispielsweise durch gezielte Phishing Angriffe oder Schwachstellen im Perimeter überwinden können, kann er sich leicht im internen Netzwerk weiterverbreiten. Auch im Falle eines internen Angreifers sollte das interne Netzwerk geschützt sein.

CYBERSEC-NG
Swiss Cybersecurity

KONTAKT

Cybersec-ng GmbH

Grünaustrasse 1

3084 Wabern

office@cybersec-ng.ch

078 729 38 39

Einsatzgebiete

Health Check

Sie sind verantwortlich für Ihre IT-Infrastruktur und/oder Applikationen und möchten einen Überblick über den Sicherheitszustand Ihrer IT-Infrastruktur und/oder Applikationen erhalten.

Kritische Systeme und Applikationen

Sie verfügen über kritische, businessrelevante Systeme und/oder Applikationen (bspw. E-Commerce), die laufend gegenüber aktuellen Sicherheitsschwachstellen geschützt werden sollen.

Firmenübernahme / Due Dilligence

Bei der Übernahme einer Firma, Software und/oder Hardware werden auch die bestehenden Sicherheitsprobleme respektive IT-Sicherheitsschwachstellen übernommen. Die Behebung der IT-Sicherheitsschwachstellen kann einen versteckten Kostenfaktor darstellen, der übersehen wird. Wir ermöglichen Ihnen IT-Sicherheitsschwachstellen sichtbar zu machen und geben entsprechende Kostenschätzungen für die Behebung der Schwachstellen ab.

Angriffssimulationen zu Übungszwecken

Sie möchten Ihr Sicherheitspersonal und Ihre Angestellten schulen und dazu regelmässige Angriffssimulationen durchführen. Die periodische Durchführung von Penetration Tests und Social Engineering Angriffen erhöht generell die Awareness der Mitarbeitenden und führt desweiteren dazu, dass im Ernstfall richtig reagiert und die entsprechenden Abläufe durchgeführt werden.