ISPIN AG ZURICH
swiss made security.®
Member of CymbiQ Group

Cyber Offensive Services

Testen Sie Ihre Umgebung, bevor ein Angreifer es tut.

Haben Sie den Sicherheitsstatus Ihres Unternehmens schon einmal mit den Augen eines Angreifers betrachtet? Wechseln Sie mit uns die Perspektive, finden Sie die Schwachstellen Ihrer Systeme und erhöhen Sie damit Ihr Sicherheitsniveau.

Cyberangriffe sind heute ein alltägliches Risiko. Kriminelle investieren viel Zeit und Know-how in die Identifikation Ihrer Schwachstellen, bevor Sie eine Attacke gegen Ihr Unternehmen starten. In der Regel genügt dafür eine Schwachstelle. Ob Sie Opfer eines Angriffs werden, hängt also massgeblich von der Frage ab, ob Ihre IT-Umgebung für Angreifer attraktiv erscheint, welche Schwachstellen sich ihnen bieten und über welchen Zeitraum diese Sicherheitslücken offen sind.

Unser ISPIN Offensive Services Team setzt für Sie die Brille eines Angreifers auf und nutzt seine Erfahrung und sein Wissen, um die Schwachstellen in Ihren Systemen zu identifizieren. Mit den daraus resultierenden Handlungsempfehlungen haben Sie die Möglichkeit, die Widerstandsfähigkeit Ihres Unternehmens zu erhöhen.

Ihre Vorteile auf einen Blick

- Erhöhung des Sicherheitsniveaus Ihres Unternehmens
- Identifikation der Schwachstellen inkl. Handlungsempfehlungen
- Prüfung Ihres gesamten Netzwerks oder einzelner Systeme
- Analyse Ihrer Infrastruktur, Ihrer Anwendungen und Informationsbeschaffung aus Sicht eines Angreifers
- Zertifizierte Methoden und Werkzeuge, z. B. PCI, NERC, CIP, OWASP
- Black-, White- und Greybox-Testing
- Interne und externe Penetrationstests

Den Hackern einen Schritt voraus.

Die Folgen einer erfolgreichen Cyberattacke sind in der Regel immens. Der ISPIN Offensive Service nimmt alle Einflussfaktoren auf die Sicherheit in Ihrem Unternehmen genauestens unter die Lupe: Applikationen, Systeme, Netzwerke und Benutzer. Dabei wenden wir dieselben Methoden und Werkzeuge an, die auch Cyberkriminelle für ihre Machenschaften verwenden. Wir überprüfen zudem auch Informationen über Ihre Organisation, die z. B. im Dark Web bereits bekannt sind und von Angreifern jederzeit genutzt werden können. Als Ergebnis erhalten Sie einen detaillierten Überblick darüber, ob Ihr Unternehmen ausreichend gegen Angriffe, von aussen oder innen kommend, geschützt ist bzw. wo Sicherheitslücken bestehen.

Umfassende Analyse, konkrete Empfehlungen

Sie können unsere Offensive Services als Teil eines umfassenden Security Assessments in Anspruch nehmen oder als Teil Ihrer regelmässigen Compliance Anforderungen. Sie können ein ganzes Netzwerk prüfen lassen oder ein einzelnes System. Unsere Experten weisen mögliche Schwachstellen aus und liefern Ihnen umfassende und verständliche Empfehlungen. Dabei erfolgt eine Priorisierung nach Kritikalität, welche es Ihnen erlaubt, dringende Handlungsfelder rasch zu identifizieren. Bei allen Penetration Tests, die wir für Ihr Unternehmen durchführen, legen wir höchste technische Massstäbe an und orientieren uns an realistischen Szenarien für böswillige Angriffe.

Methodenmix zur Schwachstellendetektion

In diesem Prozess kommen automatisierte, halb-automatisierte sowie manuelle Methoden zum Einsatz. Eine rein automatisierte Vorgangsweise reicht uns nicht. Denn deren Scheitern bedeutet nicht, dass Angreifer auch scheitern würden. Im Gegenteil: Angreifer lasen sich davon nicht abschrecken. Daher ergänzen wir automatisierte Tools durch halb-automatisierte und manuelle Methoden. Dadurch stellen wir sicher, dass wir nicht nur bekannte Schwachstellen aufdecken, sondern auch unbekannte, welche sich aus spezifischen Gegebenheiten ergeben.

Machen Sie Ihre Mitarbeitenden fit

Das schwächste Glied im Kampf gegen Cyber Security sind Ihre Mitarbeitenden. Um die Sicherheit in Ihrem Unternehmen markant zu erhöhen, müssen Sie die Sensibilität der Mitarbeitenden erhöhen und wissen welche Ihrer Daten sich im Darknet bereits befinden.

Phishing

Viele erfolgreiche Cyberangriffe beginnen mit einer E-Mail. Überprüfen Sie das Verhalten Ihrer Mitarbeitenden und etablieren Sie eine starke Sicherheitskultur auf der Basis interner Phishing-Kampagnen. Wir führen einmalig oder kontinuierlich realistische Phishing-Angriffe mittels E-Mail und/oder SMS auf Ihre Organisation durch und zeichnen die Ergebnisse auf. Dies alles ohne jegliche Installation in Ihren Systemen.

Darkweb Analyse – Wissen was Angreifer bereits wissen

Angreifer informieren sich zunehmend über Soziale Medien und im Darkweb über mögliche Schwachstellen. Dazu gehören zum Beispiel gestohlene Benutzeraccounts oder auch interne Informationen über die Netzwerk- und/oder Applikationsarchitektur. Nicht selten werden auch sicherheitsrelevante Daten durch die eigenen Mitarbeiter in Sozialen Netzwerken geteilt. Die Summe aller verfügbaren Informationen geben einem Angreifer oftmals ein überraschend gutes Bild und erlauben sehr gezielte Angriffe. Genau das machen unsere Experten. Sie erhalten dadurch einen wertvollen Einblick in den Darkweb-Footprint Ihrer Organisation und können reagieren, bevor andere es tun.

Infrastruktur auf Herz und Nieren abklopfen

Unsere Offensive Services Spezialisten überprüfen alle Bereiche, die Hacker nutzen könnten, um Ihrem Unternehmen Schaden zuzufügen. Dazu gehören die Analyse Ihrer Infrastruktur und Ihrer Anwendungen, aber auch die Beschaffung von öffentlich verfügbaren Informationen, die genutzt werden könnten, um in Ihre Systeme zu gelangen.

Discovery Scan – die gefährlichsten Schwachstellen sind diejenigen, die man nicht kennt

Sie verfügen aktuell nur über eine eingeschränkte Sicht über die Infrastruktur und Ihre Schwachstellen? Kein Problem. Durch einen umfassenden Discovery Scan, ob intern oder extern, liefern unsere Experten Ihnen ein umfassendes Bild über Ihre Assets, einen Überblick über die Schwachstellen sowie entsprechende Empfehlungen zu derer Behebung.

Network Testing – Was Angreifer sehen

Das Network Testing fokussiert sich auf die Netzwerkumgebung, d. h. Firewalls, Router und Switches (OSI Layer 2-4). Es handelt sich in der Regel um diejenigen Systeme, welche in einem Netzwerk häufig exponiert sind und deren Schwachstellen relativ einfach erkannt und ausgenutzt werden können. Durch das Network Testing werden vor allem Schwachstellen erkannt, welche hervorgerufen werden durch:

- fehlerhafte Konfigurationen
- bekannte Sicherheitslücken in Firmware und Betriebssystemen
- mangelhaftes Hardening

Das Network Testing eignet sich sehr gut, um eine Übersicht über die Schwachstellen und deren Kritikalität innerhalb des gesamten Netzwerks zu erhalten.

Anwendungen umfassend abchecken

Web Application Testing – Was Angreifer sehen könnten

Das Web und Application Testing konzentriert sich auf interne und externe Web-Applikationen sowie auf Applikationsschnittstellen. Dabei prüfen unsere Experten, wie sich die entsprechenden Systeme verhalten und welche Möglichkeiten sie für das Umgehen von Sicherheitsmechanismen bieten. Während das Network Testing häufig auf ganze Netzwerkumgebungen angewendet wird, kommt das Web Application Testing bei spezifischen Systemen bzw. Systemgruppen zum Einsatz, wie zum Beispiel Web- und Datenbankserver oder Middleware Systeme. Auch als Teil der Sicherheitsvalidierung von Systemen und Anwendungen eignet sich das Web Application Testing.

Kontinuierliches Vulnerability Management

Datacenter & Netzwerke

Sie möchten gerne fortlaufend über bestehende und neue Schwachstellen in Ihrer Systemumgebung sowie deren Kritikalität informiert sein? In diesem Fall empfehlen wir unser Vulnerability Management Service. Dabei richten unsere Experten ein fortlaufendes Vulnerability Scanning auf der externen und/oder internen Systemumgebung ein und informieren Sie beim Auftreten von Schwachstellen und Empfehlungen zu derer Behebung. Ein regelmässiges Reporting gibt Ihnen zudem eine Übersicht über den Sicherheitsstatus Ihrer Umgebung und liefert Hinweise darauf, wie rasch Schwachstellen geschlossen werden. Der Vulnerability Management Service sorgt dafür, dass Fehlkonfigurationen, ungenügendes Hardening oder bekannte Schwachstellen rasch entdeckt und somit auch behoben werden können, bevor sie durch Dritte ausgenutzt werden. Damit entlasten Sie nicht nur Ihre IT- und Security-Teams, sondern steigern auch signifikant das Sicherheitsprofil Ihrer Organisation.

Cloud Dienste

Unternehmen verlassen sich zunehmend auf Cloud Dienste von AWS (Amazon Web Services) und Microsoft Azure und gehen dabei häufig automatisch davon aus, dass sich diese Anbieter fortan um den Schutz von Daten und Applikationen kümmern. Tatsächlich merken die Unternehmen zu spät, dass dies nicht oder nur sehr begrenzt der Fall ist. Schwachstellen in der Cloud bieten daher zunehmend ein beliebtes Einfallstor für Angreifer. Die Schwachstellenerkennung in der Cloud gehört daher weiterhin zu einer effektiven Sicherheitsstrategie und deshalb überwachen unsere Spezialisten Ihre Cloud-Umgebung auf die Einhaltung der Sicherheitsvorgaben, prüfen neue Assets, verfolgen jegliche Schatten-IT und entdecken Fehlkonfigurationen.

Containersicherheit für Docker

Die Einführung von Containern für das Packen und Senden von Anwendungen revolutioniert die Software-Entwicklung. Obwohl Container isoliert sind, teilen sie dieselben Betriebssysteme, Bins und Bibliotheken mit anderen Plattformen und Anwendungen. Unsere Spezialisten sind in der Lage mögliche Schwachstellen in den Konfigurationen fortlaufend zu erkennen damit sie auch für diese Anwendungen den besten Schutz gewährleisten können.

Security Testing als Teil Ihrer Security Compliance

Security Testing ist Bestandteil vieler regulatorischer Anforderungen. Zu diesem Zweck arbeitet unser Expertenteam mit zertifizierten Methoden und Werkzeugen, welche diesen Anforderungen genügen. Dies umfasst PCI, NERC CIP, FISMA, HIPAA, OWASP, NIS Directive und Cyber Scope.

Sie benötigen kurzfristig Hilfe:

Ihre Incident Response Hotline: 0848 800 017

Cyber-Security – Swiss made und auf Ihre Bedürfnisse zugeschnitten.

ISPIN ist ein führender Schweizer Anbieter für Lösungen in Cyber Security und Cyber Risk Resilience.

Kunden profitieren von einem lückenlosen Spektrum an Beratungs- und Lösungskompetenz: Security Awareness & Culture, Governance, Risk & Compliance (GRC) gehören ebenso dazu wie Cyber Defense Services, Cloud Security Services und Sicherheitsinfrastrukturen.

Mehr als 150 Kunden aus allen Segmenten der Privatwirtschaft und der öffentlichen Hand vertrauen ISPIN. Im modernsten Cyber Defense Center der Schweiz betreibt und überwacht ISPIN rund um die Uhr die Infrastrukturen von namhaften Unternehmen, Organisationen und Behörden.

Wollen Sie mehr über unsere Offensive Services erfahren?
Wir beraten Sie gerne: cybersecurity@ispin.ch

ISPIN AG
Grindelstrasse 6
CH-8303 Bassersdorf
Tel.: +41 44 838 31 11
www.ispin.ch

Mitglied von:

FIRST Improving Security Together