DE

kapsch challenging limits

Kapsch BusinessCom

Achtung! Das ist eine Übung!

Kapsch Red Teaming: Cyber-Attacken realitätsnah simulieren.

Code Red! Das Red Team von Kapsch im Kampf gegen Cyberkriminelle. Trojaner, Spyware, Phishing, Spoofing, Social Engineering – die Methoden, IT-Systeme anzugreifen, sind mittlerweile fast unendlich. Die Antwort darauf: Red Teaming von Kapsch. Dabei schlüpfen IT-Security-Experten von Kapsch, das sogenannte Red Team, in die Rolle eines Hackers und seiner Freunde. Natürlich mit Wissen der Auftraggeber. Simuliert werden dabei alle möglichen Angriffsszenarien. Realitätsnah und unter Einbeziehung der aktuellsten Trends.

Kapsch Red Teaming im Überblick:

Red Teaming

- Ist die Königsdisziplin der IT-Security
- Erfordert ein Höchstmaß an Wissen, Kompetenz und Erfahrung, um IT-Angriffe realitätsnah zu simulieren
- Bietet ein umfassendes Szenario vieler verschiedener Angriffsmöglichkeiten
- Bezieht aktuellste Cybercrime-Entwicklungen mit ein

Warum das Red Team von Kapsch so effektiv ist:

- Das Red Team von Kapsch profitiert von der langjährigen Erfahrung der Kapsch Security-Audit-Abteilung
- Enge Zusammenarbeit des Red Teams und des Kapsch Cyber Defense Centers (CDC): Aktuelle Entwicklungen und Angriffstechniken werden im CDC beobachtet, erkannt, laufend analysiert und dokumentiert
- Umfassende internationale Zertifizierungen und Security-Expertisen
- Ständige Weiterbildung des Red Teams von Kapsch garantiert ein State-of-the-Art-Niveau von Wissen und Kompetenz

Basic Security

- Automatisierte interne Scans
- Externe Audits
- Security-Awareness-Schulungen

Standard Security

- Interne Audits
- Security Audits für Cloud-Umgebungen
- Security Audits für Produktions-umgebungen
- Social Engineering

Advanced Security

- Red Teaming

**Red-Teaming-Simulationen finden über einen Zeitraum von mehreren Monaten statt.
Der betroffene Personenkreis kann die Angriffspunkte nicht vorhersehen.**

Operative IT-Security-Ziele optimal erreichen. Ein Fall für das Red Team von Kapsch.

Die Zahlen sind beeindruckend und erschreckend zugleich: Daten des Weltwirtschaftsforums beziffern die weltweiten Schäden durch IT-Angriffe auf über 2,7 Billionen Euro. Durchschnittlich 140 Tage tummeln sich Angreifer vor einer Erkennung in internen Netzwerken. Laut Microsoft liegt der durchschnittliche Kostenaufwand im Zusammenhang mit IT-Sicherheitsvorfällen für Unternehmen bei 13,5 Millionen Euro. Fazit: Sensibilisierung ist gefragt – und vor allem Handeln. Für Unternehmen ist es maßgeblich, IT-Systeme nachhaltig zu schützen. Neben den klassischen IT-Security-Methoden sind die neuen sogenannten Red-Teaming-Übungen eine hervorragende Ergänzung zur Verbesserung der Unternehmenssicherheit.

Das Red Team von Kapsch schlüpft in die Rolle eines fiktiven Angreifers.
Beim Red Teaming geht es darum, die Widerstandskraft eines Unternehmens gegen komplexe, umfassende und möglicherweise spezifisch zielgerichtete Angriffe auf IT-Systeme und IT-Infrastrukturen nachhaltig zu erhöhen. Verteidigungsmaßnahmen, Strategien und Entscheidungsprozesse im Zusammenhang mit der Abwehr von Cyberangriffen werden auf Herz und Nieren geprüft. Das Red Team von Kapsch übernimmt dabei die Rolle eines fiktiven Angreifers: Es versucht – nach definierten Zielvorgaben – mit unterschiedlichen Methoden technischer und physischer Natur in die IT des beauftragenden Unternehmens einzudringen und sie zu kompromittieren.

Top Secret! Nur ein kleiner Personenkreis ist eingeweiht.
Das Red Team muss – wie ein realer Angreifer – unbeobachtet und in aller Ruhe über einen vorab definierten längeren Zeitraum „arbeiten“ können. Nur ein kleiner Personenkreis auf Seiten des beauftragenden Unternehmens weiß überhaupt, dass im Unternehmen eine Red-Teaming-Übung stattfindet. Nur so können technologische, systemimmanente, technisch-physikalische und menschliche Schwachstellen im Unternehmen erkannt werden.

Ziel von Red Teaming: vorab definierte und vereinbarte operative IT-Sicherheitsvorgaben prüfen.

Kapsch Red Teaming: So funktioniert es konkret.

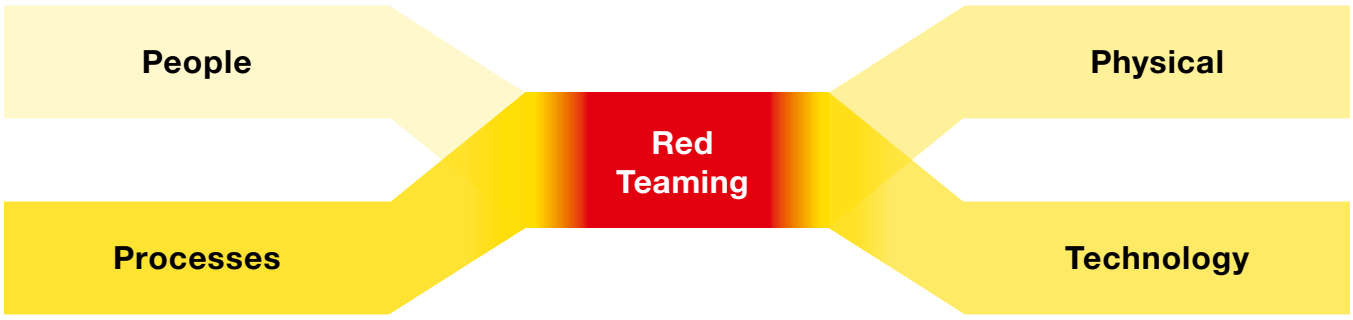
Ziele definieren.
Red Teaming beginnt grundsätzlich mit der Definition der operativen Ziele. Was will das beauftragende Unternehmen? Was empfehlen die IT-Security-Experten von Kapsch? Wo sind Schwachstellen bereits offensichtlich? An welchen Stellen gibt es Vermutungen? Der zielorientierte Ansatz von Red Teaming stellt eine hohe Realitätsnähe sicher. Welche Ziele vereinbart werden, hängt unter anderem von der jeweiligen Branche ab: Bei einem Fertigungsunternehmen ist die Lage anders als bei einem Finanzdienstleister. Ziele können eingeteilt werden in strategische Ziele und in operative Ziele.

Zielvorgaben sind zum Beispiel:

- Simulation des Zugriffs auf Kundendatenbanken
- Simulation des Kopierens von Dokumenten
- Simulation des Auslesens von E-Mail-Kommunikation (z. B. der Geschäftsführung)
- Simulation des Zugriffs auf das SWIFT-Transaktionsnetzwerk (Banken)

Der zeitliche Rahmen.
Die zeitliche Komponente unterscheidet sich vom klassischen Security Audit erheblich. Herkömmliche Audits werden in einem eher kurzen Zeitraum und am Stück durchgeführt. Red-Teaming-Simulationen finden dagegen über mehrere Wochen oder sogar Monate hinweg statt. Der Grund: Im zu testenden Unternehmen soll man ganz bewusst im Unklaren darüber sein und bleiben, wann und wo der nächste Angriff auf die IT stattfindet. Und natürlich wird auch beobachtet und geprüft, in welcher Weise und in welcher Zeitspanne die IT-Sicherheitsverantwortlichen im Unternehmen auf die Angriffe reagieren. Auch die Durchführung von Angriffen außerhalb der Geschäftszeiten ist typisch für Red Teaming.

Die Sicherheitsebenen.
Bei Angriffssimulationen werden die Targets durch das Red Team selbst ausgewählt. Der Fokus liegt dabei zunächst auf der Überprüfung jener IT-Bereiche, die auch von tatsächlichen Angreifern bevorzugt werden. Das Red Teaming umfasst vier Sicherheitsebenen: Neben der technischen sind vor allem die menschliche Ebene (Human Factor, Social Engineering), die organisatorische Ebene und die physische Ebene (Türen, Zugänge) von Bedeutung. Alle diese Faktoren werden beim Red Teaming ganzheitlich betrachtet.



Der Endbericht.
Nach Abschluss des Red-Teaming-Prozesses werden sämtliche ausgenutzte Schwachstellen dokumentiert und entsprechende Handlungsempfehlungen gegeben. Von besonderer Bedeutung ist dabei die enge Kooperation mit den IT-Verantwortlichen des beauftragenden Unternehmens. Gewonnene Erkenntnisse werden gemeinsam abgeglichen: Warum wurden gewisse Angriffe nicht erkannt? Wo gibt es blinde Flecken im System? Wo liegen Verbesserungspotenziale? Und: Welche Maßnahmen und Prozesse konnten dazu führen, Angriffe zu verhindern?

Red Teaming: Was ist zu beachten? Für welche Unternehmen ist es geeignet?

Red-Teaming-Übungen finden in enger Abstimmung zwischen dem beauftragenden Unternehmen und Kapsch statt. In einem Teamprozess definieren die (wenigen) jeweils Verantwortlichen die operativen Ziele und die Eckpunkte der grundsätzlichen Vorgehensweise.

- Wichtig ist ein gewisses Basis-Niveau an IT-Sicherheit und eine Aufgeschlossenheit für das Thema generell.
- Sollten noch keine IT-Security-Überprüfungen im Unternehmen stattgefunden haben, zum Beispiel des internen Netzwerkes oder der Internetpräsenz, sollte dies noch vor einer Red-Teaming-Übung nachgeholt werden.
- Im beauftragenden Unternehmen sollte bereits die Möglichkeit gegeben sein, Angriffe auf die IT zu erkennen: Die schnelle Erkennung und eine möglichst kurze Verweildauer von Angreifern im Netzwerk sind wichtige Ziele und werden im Rahmen einer Red-Teaming-Übung getestet.

Mit Sicherheit richtig!
Unternehmen der Finanzbranche sind (auch aufgrund europäischer Sicherheitsrichtlinien) Vorreiter beim Red Teaming. Allerdings wird der Einsatz von Red Teaming allen Unternehmen mit erhöhten Schutzanforderungen empfohlen. Mit der Einführung der österreichischen NIS-Richtlinie (NIS = Netzwerk- und Informationssicherheit) werden Red-Teaming-Überprüfungen insbesondere Betreibern von kritischer Infrastruktur empfohlen, etwa Energieversorgungsunternehmen.

Auch Red Teaming hat Grenzen.
Beim Red Teaming geht es darum, so echt und realitätsnah wie möglich potenzielle Angriffsszenarien durchzuspielen und auf ihre Wirkmacht zu testen. Doch das Red Team darf bei seinen Einsätzen nicht alles, es gibt gewisse Grenzen, auch rechtliche Bestimmungen müssen selbstverständlich eingehalten werden. So dürfen bei den Red-Teaming-Übungen vor allem keine Techniken eingesetzt werden, die geeignet wären, das Persönlichkeitsrecht zu verletzen. Das heißt: Es dürfen keine widerrechtlichen Filmaufnahmen durchgeführt oder private Laptops, Smartphones oder Tablets kompromittiert werden. Da beim Red Teaming auch „Intruding“ eingesetzt wird, also das physische Eindringen des Red Teams in sicherheitsrelevante Bereiche, gilt zum Beispiel die Regel, keine Fensterscheiben zu zerstören, um ein solches Eindringen zu ermöglichen. Ausnahme: Wenn in den Ziel- und Handlungsvorgaben ein solches Vorgehen ausdrücklich festgelegt ist.

Kapsch BusinessCom

Kapsch BusinessCom ist ein Unternehmen der Kapsch Group und unterstützt als führender Digitalisierungspartner Unternehmen bei der Steigerung der Business Performance und Entwicklung neuer Geschäftsmodelle. Kapsch agiert dabei als Berater, Systemlieferant und Dienstleistungsanbieter. Mit seinem umfassenden Know-how im Umgang mit großen Datenmengen und Security sowie einer Vielzahl erfolgreicher Use Cases in zahlreichen Branchen ist Kapsch BusinessCom der ideale Begleiter bei der digitalen Transformation. Das umfangreiche Portfolio in Österreich, Rumänien und der DACH-Region umfasst Technologielösungen für intelligente und vor allem sichere ICT-Infrastruktur, smarte Gebäude-, Medien- und Sicherheitstechnik sowie Outsourcing-Services. Kapsch setzt dabei auf Herstellerunabhängigkeit und Partnerschaften mit weltweit führenden Anbietern wie HPE, Cisco oder Microsoft sowie auf ein breites Netzwerk aus Partnern aus der Forschung und branchenspezifischen Lösungsanbietern - vom Start-Up bis zum Großkonzern.
Die Kapsch BusinessCom Gruppe hat über 17.000 Kunden – z.B. Allianz, Erste Bank, ÖBB, OMV, ORF oder Vodafone – und betreut diese lokal und global. 1.330 Mitarbeiterinnen und Mitarbeiter der Kapsch BusinessCom Gruppe erzielten im Geschäftsjahr 2018/19 einen Umsatz von rund 377 Mio. Euro.

>>> www.kapsch.net

Kapsch BusinessCom | Wienerbergstraße 53 | 1120 Wien | Österreich | T +43 50 811-0 | kbc.info@kapsch.net | www.kapsch.net

PROS-RedTeam20