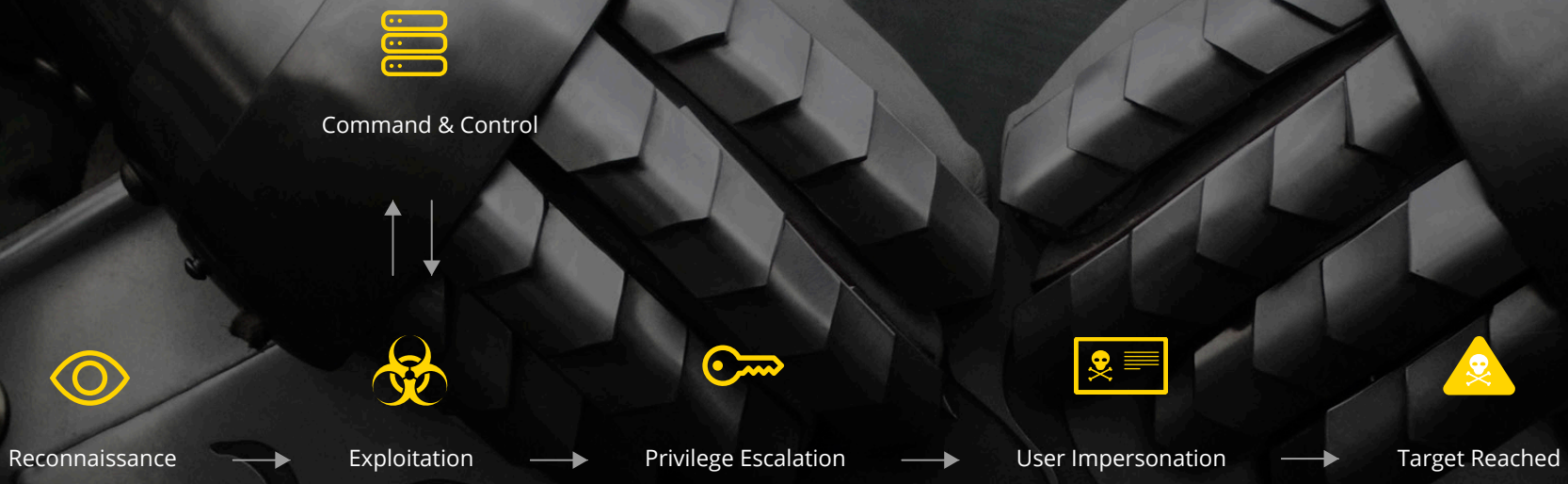
Offensive Security Services

Ein modernes Unternehmen muss heutzutage in Technologien der Cyber Security investieren. Allerdings sind Technologien allein nicht die einzige Antwort auf die aktuellen Herausforderungen. Eines der größten Probleme ist es, wirkliche Visibilität und Klarheit über eigene, explizite Sicherheitsdefizite zu erlangen. Denn nur auf diese Weise kann überprüft werden, ob alle Sicherheitsmaßnahmen intakt sind und adäquaten Schutz bieten. Für die Frage „Ist die Widerstandsfähigkeit zielgerichtet und nachhaltig in Ihrem Unternehmen gewährleistet?“ sind wir als DTS absolute Experten. Wir bieten Ihnen unterschiedliche Cyber Security Assessments an, welche unsere erfahrenen, zertifizierten IT-Experten in die Rolle eines Angreifers versetzen. Durch die Simulation von realistischen und hoch aktuellen Angriffen wird Ihr Unternehmen auf die Probe gestellt, um tatsächlich bestehende Sicherheitslücken aufzudecken.

Einzelne, unterschiedliche Assessment-Typen, z. B. Vulnerability Assessments, Penetration Tests, Red & Purple Team Engagements sowie deren hoch technische Ergebnisse sind die eine Sache. Die andere Sache ist die Kombination dieser Verfahren, das Darstellen der Ergebnisse in aussagekräftigen Reports und das anschließende Ableiten von Handlungsempfehlungen.



Wir ermitteln Ihre Sicherheitslücken durch diese Kombination und helfen Ihnen dabei zu verstehen, welchen Schaden einzelne oder verkettete Schwachstellen in Ihrem Business-Umfeld anrichten können. Auf der Grundlage dieser Sicherheitsanalysen können wir anschließend für Sie eine klare Cyber Security Roadmap entwickeln, um Ihre Cybersicherheit maßgeblich zu verbessern. Wir bauen Ihr Sicherheitsfundament, auf dem Daten, Konten, IT-Systeme und Netzwerke mit führenden Verteidigungs-maßnahmen und -mechanismen abgesichert werden können.

Unsere Cyber Security Assessments:

Internal Cyber Security Assessment
Interne Sicherheitsbetrachtung durch Anwendung des Assume-Breach-Ansatzes sowie Identifizierung von Angriffs- und Ausbreitungsmöglichkeiten von Attacken, um das mögliche Schadenspotential zu ermitteln. Dabei werden Schwachstellen und Fehlkonfigurationen analysiert und Sicherheitssysteme auf die Probe gestellt.

External Cyber Security Assessment
Tiefgreifende Überprüfung der extern verfügbaren Systeme, durch aktives Eindringen und Sammeln öffentlich verfügbarer Unternehmensinformationen sowie Aufdecken von Schwachstellen und Fehlkonfigurationen.

Web App Assessment
Umfassende Überprüfung komplexer Webanwendungen, der verbundenen Infrastruktur sowie applikationsspezifischer Berechtigungen und Rollenkonzepte.

Phishing Assessment
Analyse der Anfälligkeit Ihres Unternehmens für verschiedene Phishing-Angriffe.

Vulnerability Scanning
Erfassen der Schwachstellen Ihrer internen IT-Systeme, inkl. Priorisierung, Reporting, Handlungsempfehlungen.

Internal Cyber Security Assessment
Die Frage lautet nicht mehr ob man Opfer eines Cyberangriffs wird, sondern wann das eigene Unternehmen betroffen ist. Mit dem Internal Cyber Security Assessment bieten wir den ultimativen Cyber Security Kickstart. Basierend auf vorge-gebenen Zielen, z. B. privilegierte Konten zu kompromittieren oder sensible Datenbank-Inhalte zu exfiltrieren, wird ein Assume-Breach-Szenario abgebildet. Ein Angreifer mit Zugang zum internen Netzwerk ermittelt das mögliche Schadenspotenzial nach einer erfolgreichen, initialen Kompromittierung Ihres Unternehmens.

Ein wichtiger Bestandteil ist dabei natürlich das Herzstück: das Active Directory. Aber auch das gesamte Firmennetzwerk, die IT-Systeme und sämtliche Konten werden geprüft. Als Ergebnis liefern wir Ihnen Schwachstellen (z. B. Berechtigungs-probleme, geknackte Benutzerkonten, Sicherheitslücken auf Systemen und im Netzwerk), Korrelationen von Schwachstellen und Risikokonfigurationen aller Art (um Angriffspfade zu sensiblen Systemen, Daten oder Benutzerkonten aufzuzeigen) sowie langfristige Maßnahmen (weitere Planung der Sicherheitsinfrastruktur, um diese effizient zu verbessern).

Die Identifikation der Sicherheitslücken ist ein Aspekt. Ein weiteres Element ist, dass wir Ihnen aufzeigen, welche Angriffsmöglichkeiten tatsächlich existieren und wie diese entsprechenden Lücken ausgenutzt werden können. Das Verständnis dafür, wie Angriffsszenarien wirken und sich z. B. Malware verbreitet, kann den ent-scheidenden Unterschied ausmachen.

Was sind die DTS USP's? Zum einen agieren wir selbst wie ein Angreifer. Zum anderen ermöglichen wir es, durch die Kombination der besten Effekte verschie-dener Verfahren, hoch technische Ergebnisse zu verwerten. Damit können sowohl kurzfristige als auch langfristige, fundierte Maßnahmen abgeleitet werden. Zudem ist es möglich, eine nachhaltig langfristige Planung für eine unternehmens-spezifische Cyber Security Roadmap zu entwickeln.

- Herstellerunabhängige Analyse
- Potenzielle Angriffspunkte erkennen & verstehen
- Verbesserte Transparenz bzgl. kritischer Risiken
- Bereitstellung konkreter Handlungsempfehlungen für die Unternehmenssicherheit
- Kundenindividuelle Priorisierung der Schwachstellen
- Internes Netzwerk-Assessment, inkl. Vulnerability Assessment
- Sicherheitsüberprüfung von Services im Netzwerk
- Active Directory Assessment, inkl. Passwort-Audit
- Identifizierung von kritischen Angriffspfaden

Sie profitieren insbesondere vom DTS Internal Cyber Security Assessment, wenn …

… Sie unsicher sind, wie hoch Ihr aktuelles Sicherheitslevel ist.
… Sie Ihre Cyber-Sicherheitslücken verstehen wollen.
… Sie angemessene und wirksame Maßnahmen zum Schutz des Unternehmens ergreifen wollen.
… Sie einen Aktionsplan benötigen, um Ihre Abwehrmaßnahmen im Bereich der Cybersicherheit zu stärken.
… Sie den ROI Ihrer Ausgaben für die Cybersicherheit maximieren möchten.
… Sie sich nicht sicher sind, welche Cybersicherheitsprojekte zu welchem Zeitpunkt durchgeführt werden sollten.

External Cyber Security Assessment
Sie wollen verstehen, welche Techniken ein Angreifer anwenden kann und ob Ihre extern verfügbaren Systeme sicher betrieben werden? Das External Cyber Security Assessment ist die Antwort auf diese Frage. Die DTS Offensive Security Researcher schlüpfen in die Rolle eines externen Angreifers und sammeln öffentlich verfügbare Informationen über Ihr Unternehmen, z. B. Zugangsdaten aus historischen Data-Breaches, Domain-, System- und Benutzerinformationen. Verfügbare Systeme werden auf Schwachstellen und Fehlkonfigurationen geprüft und es wird versucht, Zugang zu Systemen oder sensiblen Inhalten zu erlangen mit dem Ziel den Perimeter zu überwinden und in Ihr Unternehmen digital einzubrechen.

- Herstellerunabhängige Analyse
- Potenzielle Angriffspunkte erkennen & verstehen
- Verbesserte Transparenz bzgl. kritischer Risiken
- Bereitstellung konkreter Handlungsempfehlungen für die Unternehmenssicherheit
- Externer Netzwerk Penetration Test
- Simulation von realistischen Angriffen

Web App Assessment

Nahezu alles ist heute eine Web Applikation oder API (Application Programming Interface). Smartphone Apps, welche via API Daten austauschen, Web-Shops oder ähnliche Anwendungen sind öffentlich zugänglich über webbasierte Protokolle. Doch sind diese auch sicher vor unerwünschtem Zugriff bzw. Handlungen?

Gartner prognostiziert, dass API-Angriffe zum häufigsten Angriffsvektor werden und Datenverletzungen in Webanwendungen von Unternehmen verursachen werden. Viele bekannte API-Schwachstellen haben bereits eine Vielzahl von Organisationen beeinträchtigt.

Die DTS Cyber Security Researcher identifizieren Sicherheitslücken in dem für Sie angemessenen Testszenario. Ob Blackbox, Greybox oder Whitebox Test, ein tiefgreifendes Web App Assessment ist unverzichtbar, um relevante Schwachstellen gemäß Web App Penetration Test (OWASP) aufzudecken und mögliche Rollenkonzepte innerhalb der Applikation auf die Probe zu stellen.

Fehlfunktionen im Access Control oder Code-Injection Angriffe stellen oftmals das größte Einfallstor für Angreifer dar, um Zugang zum System zu erlangen. Aber auch Nutzer der Webanwendung müssen angemessen geschützt werden, um zu verhindern das sich ein böswilliger Angreifer Sicherheitslücken zu Eigen macht.

- OWASP
- Tiefgreifende Überprüfung einer komplexen Webanwendung
- Überprüfung der verbundenen Infrastruktur (Datenbank, Frontend Server, Backup)
- Überprüfung von applikationsspezifischen Berechtigungen & Rollenkonzepten

Phishing Assessment
45 % aller Nutzer*innen klicken auf Links in E-Mails, auch von unbekannten Absendern.

74 % aller Unternehmen weltweit werden min. 1x pro Jahr Opfer von gezielten Phishing-Attacken.

92 % aller Cyber-Angriffe beginnen mit einer Phishing-Mail.

E-Mails sind das größte Einfallstor für Schadsoftware oder Ransomware. Mit unserem DTS Phishing Assessment bieten wir Ihnen die Möglichkeit, die Anfälligkeit Ihres Unternehmens für verschiedene Phishing-Angriffe festzustellen. Im Rahmen der gezielten, mit Ihnen abgestimmten Kampagne, führen wir einen simulierten, aber realistischen Phishing-Angriff auf Ihr Unternehmen durch und werten die Ergebnisse gemeinsam mit Ihnen aus, um anschließende Schutzmaßnahmen zu definieren. Dabei überprüfen wir ebenso den „Faktor Mensch“ und sein Sicherheitsbewusstsein. Wir zeigen auf, wie die Unaufmerksamkeit oder Gutgläubigkeit der Mitarbeitenden Ihres Unternehmens ausgenutzt werden kann und ermitteln den weiteren Schulungsbedarf.

- Analyse der Anfälligkeit Ihres Unternehmens für verschiedene Phishing-Angriffe
- Gezielte Kampagne für simulierten, realistischen Phishing-Angriff
- Auswertung der Ergebnisse & Definition von Schutzmaßnahmen
- Überprüfung des „Faktors Mensch“ bzw. des Sicherheitsbewusstseins Ihrer Mitarbeitenden

Vulnerability Scanning

Kennen Sie den aktuellen Patch-Zustand Ihrer Assets im Unternehmen? Mit dem DTS Vulnerability Assessment bieten wir Ihnen die Möglichkeit, eine Momentaufnahme der aktuellen IT-Hygiene zu machen. Die Identifizierung von System- und Software-Schwachstellen ist eines der grundlegendsten Möglichkeiten, eine erste Risiko-bewertung der eingesetzten Assets zu erhalten. CVE's (Common Vulnerabilities and Exposures), aber auch risikobehaftete Konfigurationen, werden kategorisiert und priorisiert erfasst sowie übersichtlich in entsprechenden Reports für Sie aufbereitet. Hierbei liegt der Fokus eindeutig darauf, Ihnen die Informationen effizient und leicht verständlich aufzuzeigen.

Natürlich liefern wir Ihnen ebenfalls mögliche Empfehlungen zur Schließung der Sicher-heitslücken in Kombination mit einer hochgradig akkuraten Priorisierung durch Threat Research (Häufigkeit und Schwierigkeitsgrad der Ausnutzung) sowie weiteren Faktoren. Damit unterstützen wir Sie maßgeblich auch beim effektiven Schließen der erfassten Schwachstellen.

- Einmaliges Erfassen der individuellen Schwachstellen Ihrer internen IT-Systeme (Software-Schwachstellen & Risikokonfigurationen)
- Ihre IT-Hygiene in einer Übersicht
- Schwachstellenanalyse & -priorisierung
- Reporting, inkl. Vorstellung & Beratung sowie Plan zur Remediation
- Durchführung einer Netzwerkschwachstellen-Analyse oder ganzheitliche Systemanalyse mittels Authentifizierung durch bereitgestellte Anmeldedaten
- Erfasste Informationen werden durch uns aufbereitet & in Form eines Reports, inkl. Beratung & Vorstellung der Daten, an Sie übermittelt
- Erstellung, Bereitstellung und Vorstellung der Reports für Sie

DTS Systeme GmbH
+49 5221 1013-000

DTS Systeme Münster GmbH
+49 251 6060-0

dts.de
info@dts.de