Unser kompetentes Team hat verschiedenste Angebote und Möglichkeiten sich an Ihre Wünsche bei Sicherheitstests sowie Penetrationstests anzupassen. Die folgenden Angebote sind speziell gewählt und extra auf den jeweiligen Kunden zugeschnitten der unser Angebot in Anspruch nimmt.

Externer Penetrationstest:

Ihr Unternehmen setzt einen hohen Wert auf Web und Netzwerk Sicherheit?
Sie benötigen Hilfe zum Absichern ihrer Systeme und betrieblichen Server?

Wir helfen Ihnen dabei und machen einen kompletten Sicherheitscheck rund um alle Web-Services & Dienste, die Sie auf Ihrer Internet-Präsenz anbieten. Wir geben Ihnen qualitative Verbesserungsvorschläge und Anweisungen in Form von Analyse-Papers, in denen Sicherheitslücken und andere Schwachstellen am System offen gezeigt und verständlich für Ihre Mitarbeiter und Administratoren dargestellt werden.

Für einen externen Test benötigen wir lediglich ihre Internetadresse, um einen Test durchzuführen. Die Techniken & Methoden mit denen wir vorwiegend arbeiten, fallen meistens in den manuellen Anwenderbereich und nicht in automatisierte Scripte oder Schadsoftware die überall für Jedermann zum download abrufbar ist. Ein externer Penetrationstest zielt also hauptsächlich nur auf die im Web(WWW) erreichbaren Services. Unser kompetentes Team versucht also von außen Ihr System zu penetrieren und verbessert so die Sicherheits-infrastruktur Ihrer Firma.

Interner Penetrationstest:

Ihr Unternehmen ist daran interessiert, was im Netzwerk an Sicherheitslücken Ihre Infrastruktur von innen heraus zerstören könnte? Ihr Unternehmen ist gezwungen einen administrativen Sicherheitscheck im internen Netzwerk zu organisieren?

Wir vernetzen uns gerne mit Ihren privaten oder öffentlichen Firmen-Netzwerken und testen einzelne Arbeitsplätze, sowie alle im Netzwerk erreichbaren Server & Systeme auf Schwachstellen und Sicherheitslücken. Je nach Infrastruktur können so einfach und schnell die internen Netzwerke abgesichert werden, damit Ihre Firma ein sicheres Standbein auf dem globalen Markt vorweisen kann. Um einen schnellen und einfachen Überblick zu haben, gibt es auch für diesen Bereich Analyse-Papers, die qualitativ hochwertige Informationen enthalten. Wir testen nicht nur Ihre im Netzwerk vorhanden Services, sondern überprüfen auch gerne einzelne wichtige Computer auf Sicherheitslücken oder Schutz vor Angriffen. Gerne hören wir uns auch eigene von ihnen entwickelte Ablaufpläne an und folge diesen.

Web-Applikationen Audits:

Sie haben eine Internetseite mit einem Content Management System(CMS) oder einer Webapplikation(SHOP) in Java, HTML, HTM, PHP, ASP mit Datenbankanbindung? Ihre Firma arbeitet für eine Behörde und es ist zwingend notwendig ein vorgeschriebenes Sicherheitsmaß zu halten?

Unser Unternehmen verteidigt ihre Handelsportale, Shop-Systeme, CMS oder Kunden vor bösen Crackern indem wir ein Sicherheitskonzept abarbeiten das zahlreiche Weblücken identifiziert und im Anschluss ausschaltet. Unsere kompetenten und aufgeweckten Penetrationstester arbeiten auf hohem Niveau und meist nicht mit automatisierten öffentlichen Programmen und haben somit eine deutlich höhere Angriffsquote. Mit einfachen und effektiven Mittel identifizieren wir Schwachstellen und führen sie Ihnen im Anschluss vor.

Software (Program) Audits:

Ihre Firma arbeitet an einem eigenständigen Programm das für den wirtschaftlich offenen Markt bestimmt ist und Sie oder ihre Mitarbeiter haben keine herausragenden Sicherheitskenntnisse? Sie haben eine Software in C, Java, Delphi oder VBS die gewisse Sicherheitsvorschriften erfüllen muss?

Wir helfen ihnen ihre Software sicher und funktionsfähig zu gestalten. Wir schauen während der Implementierungsphase oder Beta-Phase ihre Produkte an und führen aktive Sicherheits-Audits and ihnen durch. Angefangen bei einfachen Eingabefehlern bis hin zu Fehlfunktionen oder Manipulationen(Crashs) decken unsere kompetenten Sicherheitsspezialisten alle erkennbaren und verdeckten Schwachstellen auf. Gerne schauen wir auch ihre Software Projektpläne an und sagen ihnen worauf sie bei einzelnen Bereichen achten müssen.

Black & White Penetrationstests:

Alle unsere Angebote im Bereich, der Penetrationstests und Sicherheitsaudit müssen in Kombination mit einem Black und White Feature in Anspruch genommen werden.

Black Penetrationstest:
Bei einem externen Black(Schwarz) Penetrationstest stehen keine Daten(Quellcode, Betriebsinformationen & Netzwerkinformation) zur Verfügung. Unser Team muss also über Umwege an Informationen und Daten kommen und diese auch kompetent nutzen um ein qualitatives Resultat zu erzielen. Im diesem Testverfahren arbeiten unsere Mitarbeiter aus der Perspektive von wirklichen Hackern/Crackern.

White Penetrationstest:
Bei einem externen White(Weiß) Penetrationstest stehen hingegen Informationen und Quellcodes, der Services und Dienste zur Verfügung. Diese Informationen betreffen z.B. die Versionsnummer einer Software, Dienstauskünfte(SSH, FTP, IMAP, TELNET) oder den Quellcode einer Applikation. Im Team kommen unsere Mitarbeiter natürlich einfacher an Lösungen und Ergebnisse um ihr System zu sichern.

Web Vulnerability Scanning:

Ihre Firma möchte vorab wissen welche Schwachstellen von außen zu identifizieren sind? Sie sind sich bei unseren Angeboten noch nicht sicher was sie brauchen und möchten gerne einen vorab „Scan“ auf Schwachstellen machen?

Wir tasten mit eigens entwickelter und frei verfügbarer Software ihre Systeme ab und senden ihnen die Resultate verständlich in einer Dokumentation mit kompetenten Lösungen und Vorschlägen zum fixen der Schwachstllen. Dieses Angebot empfehlen wir ihnen. Wir testen von einfachen Schwachstellen wie XSS Schwachstellen bis hin zu Buffer-Overflows und Format-Strings. In diesem Paket ist kein Penetrationstest enthalten lediglich der Scan mit den Resultaten und Logs.

Hacker Workshops, Events & Live-Hacking:

Ein Penetrationstest ist eine Methode von IT Sicherheitsexperten, die darauf beruht einen IT Dienst manuell oder automatisiert so zu manipulieren, dass die Software oder Applikationen ungewollte Funktionen ausführt. Immer häufiger tauchen bei Applikationen und Programme ungewollt schwere Sicherheitslücken auf, die meist erst dann offenbart werden können, wenn man über eine gewisse Erfahrung bezüglich der Problematik verfügt. Für einen erfolgreichen Anwendungsentwickler, der für ein Unternehmen arbeitet ist es zwingend notwenig, diese Kenntnisse von Zeit zu Zeit zu schulen und sich mit anderen darüber auszutauschen, damit anstehende Projekte oder Dienste nicht von außen attackiert werden können. Ein erfolgreicher Angriff auf ein Unternehmen schädigt nicht nur den Ruf, sondern kann auch bei Fahrlässigkeit ernsthafte rechtliche Konsequenzen nach sich ziehen. Wir zeigen Ihnen wie Hacker arbeiten und welchen brisanten Techniken Sie benutzen. Wir stellen Ihren Administratoren und Mitarbeitern ein innovatives und ausgeprägtes Konzept zur Verfügung, das spezifisch auf ihr Firmenprofil zugeschnitten ist.

Wir kombinieren Vorlesungen mit Live-Hacking an Applikationen sowie hochwertigen Informationsmaterialien und fördern damit das „Know-How“ ihrer Mitarbeiter. Unser Unternehmen bietet Ihnen somit die Möglichkeit, frei zu entscheiden, in welchem Bereich Ihre Mitarbeiter oder Administratoren für die tägliche Arbeit wichtige Erfahrungen sammeln sollen. Zeitlich kann eine Trainingssitzung zwischen 2-8 Stunden betragen je nach wunsch. Gerne können Sie sich telefonisch bei uns melden um sich näher über die jeweiligen Vorlesungen, Weiterbildungen, Termine sowie Preise zu informieren. In den wie folgt aufgeführten Punkten schulen wir Ihre Administratoren sowohl durch Angriffs-Szenarien als auch in Abwehrmaßnahmen und stellen dazu noch hoch qualitatives Material (White-Papers, Dokumentationen) zur Verfügung …

- Cross-Site-Request-Forgery & Cross-Site-Scripting
- Local/ Remote File-Inclusion & Directory-Traversal
- SQL-Injection, HTML-Injectionen & Gegenmaßnahmen
- Ddos Attacken, Bombing-Angriffe & Abwehrmaßnahmen
- Web-Phishing & Fake-Requests
- Module & Exploits (Frameworks & Scripts)
- Viren, Würmer, Rootkits & Trojaner
- Mail-Order Angriffe & Social-Engeneering
- Buffer Overflows & Format-Strings

Schulungen & Events:

Unsere Firma MNS bietet nicht nur Workshops sondern auch Schulungen für Administratoren und deren Mitarbeiter an. Wie auch in den anderen Themenbereichen fällt auch hier der Schwerpunkt auf IT Sicherheit. Um sich einen Überblick auf die verschiedenen Schulungen zu verschaffen haben wir extra für Sie die folgenden Informationen zusammengetragen.

- **WLAN Sicherheit** (WEP,WPA, PS Key, Angriffstechniken & Abwehrmaßnahmen)
- **IT Sicherheitstraining** (Angriffsmuster, Angriffsverfahren und allgemeine Abwehrtechniken)
- **IT Forensik** (Angriffs-Analysen, Log-Analyse & rechtlich nutzbare Auswertungen)
- **Einsteiger Penetrationstester** (Grundlagen für Penetrationstester)
- **Fortgeschrittener Penetrationstester** (Weblücken, Servicelücken, Methoden & Techniken)
- **AV & Firewall- und IDS-Management** (Grundlagen von FW Schutzmechanismen und IDSM)
- **Der Datenschutzbeauftragte** (Datenschutz, gesetzliche Aspekte & Rechtswissen)

Alle unsere Schulungen, Vorlesungen & Vorstellungen setzen kein IT Grundwissen voraus. Die Schulungen nehmen durchschnittlich 1-2 Tag in Anspruch und beinhalten kurze Pausen.

Schulungsmaterial & Dokumentationen:

Unsere Firma bietet ihren Sicherheitstechnikern, Anwendungsentwicklern, Datenschutzbeauftragten und Administratoren qualitative und ungeschnittene Sicherheits-Papers, mit Quellcodes und Informationen über Schwachstellen, Angriffsszenarien sowie Abwehrtechniken. Wir zeigen an grafischen Beispielen und realen Quellcoderückblicken wie ein Angreifer Lücken und Wege nutzt um in Systeme einzudringen.

Schulen Sie sich und ihre Mitarbeiter indem und erwerben sie unsere interessant geschriebenen Dokumente und Codes. Mit einfachsten Mitteln wird es so für Sie möglich einfache bis komplizierte Angriffs und Abwehrszenarios nachzuvollziehen und nachzuahmen.

In jeder Dokumentation liegt zusätzlich noch ein Live-Hack Video von einem Testszenario bei. Die Lizenz schränkt die Weitergabe in gewisser Anzahl an Mitarbeiter, des Firmeninhabers ein.

Arbeitsabläufe & Konzeptkreislauf:

Unser kompetentes Team bietet Ihnen eine solide Basis um in den Bereich der IT-Sicherheit einzusteigen. Unsere Services werden ständig von uns überarbeitet und weiter entwickelt um unseren Kunden ein gutes Preis-Leistungsverhältnis zu bieten. Alle der folgenden Services und Dienste bieten Wir unseren Kunden um ein hohes Maß an Sicherheit und Stabilität zu gewähren.

Penetrationstest Aufbau:

- Reconaissance (Informationsbeschaffung)
- Enumeration (Angriffs-Vektoren)
- Exploitation (Ausnutzen von Schwachstellen)
- Documentation

Konzept-Bereiche:

- Planung
- Simulation
- Ausführung

Planung & Ablauf:

Die Planung eines Abaufs ist das wichtigste was unsere Routinen umfasst da man sich in dieser Phase über Infrastrukturen und die Durchführung navigiert und organisiert.

Überblick:

Die Konzeption der einzelenen Bereiche bauen auf einander auf und führen somit am ende eines kompletten Ablaufs zu einem hervorragenden Ergebnis für den jeweiligen Auftraggeber. Nach jedem Penetrationstest werden an die jeweiligen Auftraggeber einzelne Berichte übergeben die aufweisen was gefunden, überprüft oder veranlasst werden sollte. Um einen erfolgreichen Ablauf zu gewähren passen Wir uns dem jeweiligen Kunden und seiner Infrastrukturen an und finden optimale Lösungen aus der Perspektive, des Angreifers oder Sicherheitsberaters.