



Omicron - Security Services

OMICRON AG
INDUSTRIESTRASSE 50B
P.O. Box 384
8304 WALLISELLEN
SWITZERLAND

PHONE +41 (0)44 839 11 11
FAX +41 (0)44 839 11 00
E-MAIL MAIL@OMICRON.CH
WEB [HTTP://WWW.OMICRON.CH](http://WWW.OMICRON.CH)

Wieso sind wir angreifbar?

Der Netzwerk den wir als Internet kennen war ursprünglich ein militärisches Projekt das den Anspruch hatte, Informationen von A nach B zu übermitteln, auch wenn bereits teile des Netzes zerstört sind. Weitere Sicherheitsanforderungen wurden dabei nicht gestellt. Später nutzten Universitäten diese Technologie um zu kommunizieren und sich auszutauschen. Aus diesem Netzwerk wuchs das heutige Internet mit immer neuen Anwendungen und Protokollen. Diese bauen aber alle auf dem historisch gewachsenen und sehr verbreiteten Vernetzungsgrundlagen auf. Diese offenbaren in der heutigen Anwendung konzeptionelle Schwächen, die ausgenutzt werden können. Software wird immer komplexer, die Innovationszyklen immer kleiner. Objektorientierte Programmiersprachen erlauben die Entwicklung sehr umfangreicher Software. Jedes Objekt agiert und reagiert dabei über seine eigenen Schnittstellen mit anderen Objekten. Es ist sehr schwierig und Zeitaufwendig, alle möglichen Fälle zu testen, das kann wiederum Fehler und Schwachstellen zur Folge haben, die mit der Anwendung beim Benutzer implementiert werden. Wo Menschen arbeiten, werden Fehler gemacht. Das betrifft wiederum die Programmierung aber nun auch die Installation, Konfiguration, den Betrieb und die Wartung von komplexen Systemen. Häufige Ursachen sind dabei Zeitdruck, Nachlässigkeit, mangelnde Ausbildung aber auch mangelndes Bewusstsein für die Wichtigkeit des eigenen Handelns und dessen Konsequenzen für das Unternehmen.

Omicron Security Services Definition

Unsere Sicherheitsanalysen sind massgeschneiderte Services die auf Modulen und Optionen basieren. Module können beliebig ausgewählt, kombiniert, ausgearbeitet und mit Optionen versehen werden. Daraus entsteht ein Analysekonzept, dass auf Ihre Bedürfnisse und Infrastruktur zugeschnitten ist.

Die Analysemodule

System & Network Audit

Mit einem System & Network Audit wird überprüft, ob die Systeme den gestellten Unternehmensrichtlinien entsprechen. Umfassende Richtlinien regeln, wie Systeme aufgesetzt, konfiguriert, gewartet, in das Netz eingebunden werden und mit anderen Systemen kommunizieren dürfen. Das Audit gibt Aufschluss, wie gut Richtlinien eingehalten werden, aber auch welche Problemstellungen dabei auftreten. Richtlinien müssen praktikabel sein, damit diese Beachtung finden und konsequent zur Anwendung kommen.

Infrastructure Assessment

Systeme, Anwendungen oder ganze Netze werden systematisch auf Sicherheit überprüft. Betriebssysteme und Applikationen werden nach Schwachstellen untersucht, Konfiguration und Kommunikation der Systeme analysiert. Die Richtlinien sowie das Umfeld der Systeme werden dabei berücksichtigt, jedoch steht alleine die generelle Sicherheit des Systems, der Anwendung oder des Netzes im Vordergrund.

Web Applications Assessment

Der Internetauftritt ist heutzutage Pflicht jedes Unternehmens. Der Bedarf der Kundschaft oder Geschäftspartner auf Daten online zuzugreifen ist gross, manchmal sogar wettbewerbsentscheidend. Das zu Verfügung stellen von Datenbankinhalten wie z.B. Kundendaten auf dem Web birgt viele Risiken. Sehr wichtig dabei ist ein sicheres Anmeldeverfahren, sowie eine sichere Interaktion zwischen dem Webserver zur Darstellung und der Datenbank als Datenlieferant. Die Webanwendung darf auch keine Informationen weitergeben, die einem Angreifer Hinweise geben könnte. Ein Web Applications Assessment untersucht, ob sich der Schutz der Daten, die Infrastruktur des Unternehmens, aber auch die Sicherheit des Users auf dem höchstmöglichen Niveau befinden.

Firewall Assessment

Die Firewall, die „Zollstation des Datenhighways“ als erste und wichtigste Verteidigungslinie gegen ungebetene Gäste und Abschottung betriebseigener Ressourcen. Sie ist vor dem Webserver das exponierteste System eines Unternehmens. Ein Firewall Assessment dient dazu, die richtige Konfiguration, die Qualität des „Rulesets“ und die Immunität gegen Angriffe gegen das System selbst von aussen und innen zu überprüfen. Weiter werden Dienste und die dienst anbietenden Systeme hinter einer Firewall auf Schwachstellen geprüft.

Penetration Test

Systeme, Anwendungen und Netze werden getestet um die Möglichkeiten, die ein Angreifer hätte, ausfindig zu machen. Je nach Vereinbarung können während eines Penetration Tests sogar Methoden zum Eindringen in ein System durchgeführt werden. Es handelt sich dabei also um ein reales Szenario, das jedoch im Gegensatz zu einem echten Angriff kontrolliert und unter klaren Vereinbarungen und Befugnissen abläuft. Es ist so möglich, Schwachstellen im gesamten Sicherheitskonzept zu finden.

Architecture Review

Schon bei der Architektur eines Netzes sind die Aspekte der Sicherheit zu berücksichtigen. Netze sind sehr dynamische Gebilde und befinden sich stetig im Wandel. Nach Monaten oder Jahren steht das ursprüngliche Design nur noch verschwommen da, was zu konzeptionellen Sicherheitslücken führen kann. Die Netze dienen immer mehr Anwendungen mit neuen Protokollen als Transportmedium, Kompromisse die auf Kosten der Sicherheit gehen häufen sich. Ein Architecture Review zeigt aus neutraler Sicht wo Sicherheitsprobleme aufgrund des Netzwerkdesigns auftreten können und wie man diese schliessen kann.

Die Optionen

Social Engineering

Der Mensch ist die grösste Schwachstelle. Tugenden wie Hilfsbereitschaft, Offenheit und Nettigkeit können ebenso ausgenutzt werden wie die Naivität, Ignoranz oder Fahrlässigkeit. Oft ist Mitarbeitern nicht bewusst, welche Konsequenzen die Weitergabe oder der unsachgemässe Umgang mit Informationen haben kann. Mit Social Engineering wird meist durch Telefon oder E-mail versucht, hilfreiche Informationen wie Passwörter oder Informationen zu Systemen, Plattformen und Anwendungen zu erfragen, die später für einen Angriff benutzt werden. Ein guter Hacker arbeitet die meiste Zeit ohne Computer.

Extended Information Gathering

Das Internet ist heute eine der wichtigsten Quellen von Informationen aller Art. Die Homepages von Firmen beinhalten eine Fülle von Informationen, die sehr viel über die Organisation, die technische Infrastruktur und das Sicherheitsbewusstsein der Firma verraten oder zumindest erahnen lassen. Auch Einzelpersonen, egal ob privat oder beruflich motiviert, stellen Informationen in das World Wide Web. Diese oft detaillierten Inhalte können einem Angreifer ein umfangreiches Bild, z.B. über die Ausbildung, Engagement und Erfahrung von IT Personal und Management oder wichtige Anhaltspunkte für "Brute-Force"-Attacken auf Systeme von Benutzern geben.

Warwalking

Firmen kriegen täglich Besuch von allen möglichen Leuten. Der Postbote, der Kurier, der Vertreter, der Kunde, das Reinigungspersonal, der Lieferant, der Heizungsmonteur, der Installateur usw. Einem Mann im Overall eines bekannten Kurierdienstes mit vielen Paketen im Arm hält man hilfsbereit die Türe auf, denn jeder kann ja sehen das es sich hier um den Kurier handelt, was denn sonst - oder doch nicht? Mit einer guten Portion Dreistigkeit, Mut und ein wenig Phantasie gehen viele Türen auf. Warum durch Port 80, wenn die Türe bereits offen steht?

Wardriving

Wireless ist wirklich praktisch und davon sollte man auch profitieren. Wireless Access Points lassen sich sicher konfigurieren, wenn man weiss wie, und dies auch tut. Wireless gibt es im Büro nicht? Also bringe ich einfach meinen Access Point von Zuhause mit oder kaufe mir einen, dann sind wir endlich mobil. So kann es schnell geschehen, dass eine Firma mehr Wireless hat als vorgesehen. Diese Access Points sind nicht sicher konfiguriert und können direkten Zugang zum Intranet ermöglichen. Eine Begehung Ihrer Gebäude, Ihres Firmenareals mit einem Notebook mit Wirelesskarte, GPS Karte und entsprechender Software entdeckt alle Access Points und erstellt auch noch automatisch eine Karte. Jeder Access Point wird auf seine Sicherheit geprüft.

Generelle Vorgehensweise

Hier wird die Standardvorgehensweise beschrieben. Je nach Vereinbarung mit dem Auftraggeber wird diese entsprechend dem Auftrag angepasst.

Pre-Analysis Phase

- Welche Form von Sicherheitsanalyse soll gemacht werden
- Wo werden diese angewandt
- Was sind die Rahmenbedingungen
- Konzeption
- Festlegen der Verantwortlichkeiten
- Massgeschneiderte Offerte
- Rechtliche Aspekte

Analysis Phase

- Analyse wird nach Konzept durchgeführt
- Tägliche Briefings
- ev. Sofortmassnahmen falls notwendig

Post-Analysis Phase

- Präsentation der Resultate
- Sofortmassnahmen
- Berichte werden erstellt
- Massnahmen Plan

Re-Analysis Phase

- Überprüfung der getroffenen Massnahmen
- Bericht
- Abschluss



Wieso brauchen Sie eine externe Expertise?

Betrachtet man ein beliebiges reales Objekt wird die Aufmerksamkeit meist auf wenige Punkte gelenkt. Welche das sind ist von Betrachter zu Betrachter unterschiedlich. Erst der Austausch der verschiedenen Eindrücke macht bewusst, dass man nicht alles wahrnimmt was man sieht. Die Sicht aus anderen Perspektiven, durch andere Augen offenbart immer neues.

Es gibt meist viele Wege ein Ziel zu erreichen aber auch viele die in die Irre führen. Mittel und Methoden sind oft entscheidend wo man lang geht und ob das Ziel zu erreichen ist.

Erfahrung braucht Zeit intensive Auseinandersetzung mit der Materie, eine Spezialisierung ist daher notwendig denn der Tag hat für alle nur 24 Stunden.

Kontaktinformationen:

Omicron AG
Industriestrasse 50b
CH-8304 Wallisellen
Telefon +41 (0)44 839 11 11
Fax +41 (0)44 839 11 00
E-Mail: mail@omicron.ch
Web: <http://www.omicron.ch>

