



Omicron - Vulnerability Scan 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)

Omicron Vulnerability Scan Services – Reduzieren Sie Ihre Risiken - Erhöhen Sie Visibilität und Sicherheit

Heutige Unternehmensumgebungen basieren auf komplexen und schwer überblickbaren Netzwerk- und Systeminfrastrukturen um Geschäftsprozesse für Mitarbeiter, Kunden, Partner und Lieferanten jederzeit bereitzustellen. Diese Entwicklung zur Verbesserung der Produktivität, der Effizienz bei gleichzeitig nötigen Kosteneinsparungen stellt Systemverantwortliche vor grosse Herausforderungen. Die fast täglichen Veröffentlichungen von Verletzbarkeiten und die damit verbundenen Update- und Patch-Zyklen machen das Leben dabei nicht wirklich einfacher.

Wir helfen Ihnen durch unseren Vulnerability Scan Service in regelmässigen Abständen, oder auf Wunsch einmalig, Ihre komplette Infrastruktur aus interner sowie auch aus externer Sicht zu überprüfen und nach Risiken zu bewerten. Dabei helfen Ihnen eine detaillierte Auswertung und ein kompakter Bericht die nächsten Schritte zu planen und umzusetzen.

Ihr Nutzen auf einen Blick

- Identifikation von Verletzbarkeiten am Perimeter, aus externer Sicht, oder im Unternehmensnetzwerk, für einen internen Blickwinkel
- Betriebssystem- und Applikationskontrolle auf bekannte Schwachstellen und Verwundbarkeiten
- Überprüfung der Schutzwirkung bereits vorhandener Sicherheitslösungen
- Risikobeurteilung der Zugangsmöglichkeiten zu internen und vertraulichen Informationen und Systemen
- Validierung und Kontrolle von Systemupdates und -Patches
- Schutz der Integrität von Online-Assets wie Shopping- oder Lieferanten-Portale
- Unterstützung bei industriespezifischen Zertifikationen und Compliance-Anforderungen wie SOX, HIPAA, PCI, Basel II, etc.
- Beweisbarkeit durch klare Auswertungen und aussagekräftige Berichte
- Reduktion der Kosten und des Risikos eines Ausfalls oder einer Beeinträchtigung durch Verringerung des Angriffs- und Schadenspotenzials

Ihre Unternehmenssicherheit liegt uns am Herzen

Unsere Spezialisten verfügen über das aktuelle Fachwissen sowie die nötigen Tools und Methoden um komplexe aber auch eher seltene Umgebungen und Betriebssysteme in die Sicherheitsüberprüfung mit ein zu beziehen. Dabei setzen wir in erster Linie auf passive Kontroll- und Monitoringszenarien und schonende Verwendung der Bandbreiten, um keine Prozesse und somit in keiner Art und Weise Ihre Geschäftsaktivitäten oder Ihren Informationsfluss zu beeinflussen.

Ihre Vorteile und Leistungen

Omicron Vulnerability Scan Services	Von Extern	Von Intern
Prüfung & Identifikation von Verletzbarkeiten	Am Netzwerk Perimeter	Innerhalb des Unternehmensnetzwerks
Umfang Standard / Anzahl IP Adressen	10 IP's	Class C – 255 IP's
Durchschnittliche Scan Dauer	1 Tag	1 Woche
Detailliertes Reporting als PDF-Dokument per E-Mail	Ja	Ja
Kategorisierung der Schwachstellen nach Risiko	Ja	Ja
Vorschläge zur Verbesserung der Sicherheitsstufe	Ja	Ja
Empfehlungen zu Compliance-Anforderungen	Ja	Ja
Empfehlungen zur Umsetzung & Implementation	Ja	Ja
Installation/Anschluss von Equipment vor Ort	Nein	Ja
<i>Preisempfehlung in CHF, exkl. MwSt.</i>	<i>1'500.- Je weitere 10 IP's plus 1'000.-</i>	<i>4'500.- Je weiteres Class C Netzwerk auf Anfrage</i>

Erst die Regelmässigkeit gibt ein sicheres Gefühl

Erst eine kontinuierliche und regelmässige Überprüfung gibt Ihnen die nötige Sicherheit heute aber auch morgen über gesunde und gesetzeskonforme sowie sichere Systeme zu verfügen. Dabei macht es durchaus Sinn in definierten Abständen eine komplette Überprüfung durch unsere Fachleute und Experten durchführen zu lassen.

Unsere Empfehlung – Ihre Absicherung

Wir empfehlen bei kleinen Unternehmen eine quartalsweise oder halbjährliche Überprüfung. Bei sicherheitskritischen Systemen und grösseren Unternehmensumgebungen macht eine monatliche Überprüfung durchaus Sinn und sollte von jeder sicherheitsbewussten Firma ins Auge gefasst und budgetiert werden.

Beweisen und erfüllen Sie Ihre Compliance Anforderungen. Stehen Sie auf der sicheren Seite, wir helfen Ihnen dabei.

Gemischte Infrastrukturen – Unsere Herausforderung

Ein Auszug der einbezogenen Betriebssysteme:

BeOS, BSD generic, Caldera OpenLinux, Caldera UnixWare, Cisco IOS, Compaq True64, Conectiva Linux, Convex OS, Debian Linux, DG/UX, EnGarde Secure Linux, Fedora Core, FreeBSD, HP Apollo Domain/OS, HP-UX, IBM AIX, IBM AS/400, Immunix, IRIX, Linux based OS, Mac OS, Mandrake Linux, Microsoft Windows - Alle Versionen, NEC EWS-UX/V, NEC UP-UX/V, NEC UX/4800, NetBSD, NeXTSTEP, Novell NetWare, OpenBSD, OpenVMS, OS/2, OS-9, QNX, RedHat Linux, SCO Open Server, Slackware Linux, Solaris, SunOS, SuSE Linux, Trustix Secure Linux, Turbolinux, Ultrix, UNICOS, UnitedLinux, VxWork

Überblick der Testprozeduren und Prüfkompontenten:

Brute-Force password guessing, Backdoors, Browser CGI-Bin, Daemons, DCOM, Denial-of-service, DNS, E-Mail, Firewalls, FTP, Information gathering, Instant messaging, LDAP, NetBIOS, Network sniffers, NFS system requirements, NIS, Protocol spoofing, Router switch, RPC, Shares, SNMP, Web scan, Windows critical issues / groups / networking / password checks / password policy / patches / policy issues / registry / services / users / X-Windows

Fazit – Sichere und gute Geschäfte mit sicheren Systemen

Eine detaillierte Analyse und Auswertung zeigt Ihnen klar und übersichtlich welche nächsten Schritte dringend nötig sind um Ihre Infrastruktur vor aktuellen Bedrohungen und Gefahren abzuschotten und wie Sie gesetzliche Vorschriften einhalten und dessen Einhaltung auch beweisen können.

Gerne helfen wir Ihnen auch vor Ort bei der Umsetzung und Implementierung der empfohlenen Vorschläge.

Fragen Sie uns an und lassen Sie sich kompetent durch unsere Experten beraten. Telefon: 044 839 11 11