Bestellen Sie jetzt Ihren CGM IT-Security-Check.

CGM IT-Security-Check

Ihr Unternehmensnetzwerk bietet Zugriff auf wertvolle und geschäftskritische Informationen. Diese Informationen sollten auf keinen Fall in die falschen Hände gelangen. Sind Sie sicher, dass Ihnen böse Überraschungen, die ihre wertvollen Informationen gefährden könnten, erspart bleiben? Keine Malware, Hintertüren, Datenverluste oder andere Sicherheitsschwachstellen? Eine frühzeitige Erkennung von verborgenen Bedrohungen ermöglicht es, dass Sie diese Risiken unmittelbar adressieren und Ihr Sicherheitsniveau erhöhen können.

Mit dem CGM-IT-Security Check können Sie die Sicherheitsrisiken für Ihr Unternehmen aufdecken. Der Security-Check-up ist eine Analyse und Beurteilung der Sicherheitsrisiken, denen Ihr Unternehmensnetzwerk ausgesetzt ist. Am Ende dieser Sicherheitsüberprüfung erhalten Unternehmen einen ausführlichen, analytischen Bericht zur Bedrohungssituation. Ein Sicherheitsexperte wird diesen Bericht gemeinsam mit ihnen durchgehen. Der Bericht umfasst auch die Sicherheitsvorfälle, die während der Überprüfung Ihres Netzwerks festgestellt wurden, sowie Empfehlungen, wie Sie sich vor diesen Bedrohungen schützen können. Unsere Spezialisten geben Ihnen gerne Ratschläge, unterstützen Sie in allen Fragen der Sicherheit und helfen dabei, Ihr Unternehmen optimal abzusichern.

- Eine vergleichsweise kleine Investition, die sich auszahlt.
- Handeln Sie jetzt, denn IT-Sicherheit ist Chefsache.
- Leistungsdetails siehe Rückseite.
- Dienstleistungsaufwand: 2-3 Tage
  (je nach Größe der Einrichtung/Klinik).

CGM IT-Security-Check

Ablauf:

- Einrichtung des CGM Security-Gateways zur Erfassung der Daten.
- Analyse des Netzwerkverkehrs.
- Analyse der Ergebnisse.
- Bericht zu den Erkenntnissen.

Für den Security-Checkup stellt CGM ein Security-Gateway zur Verfügung, das den Datenverkehr im gesamten Netzwerk analysiert und untersucht. Dieses Gateway wird nicht in das Netzwerk integriert. Das Gateway analysiert den gespiegelten Netzwerk-Datenverkehr und nutzt hierfür den Monitor-Port, der mit einem Test Access Point (TAP) oder einem Mirror-Port (bzw. Span-Port) auf dem Netzwerk-Switch verbunden ist. Somit stellen sich keinerlei Herausforderungen hinsichtlich der Inline-Konnektivität, da sichergestellt ist, dass ausschließlich der kopierte Datenverkehr analysiert wird.

Inhalte und Schwerpunkte:

- Risikoreiche Web-Anwendungen und Websites, die von Mitarbeitern genutzt werden: P2P-File-Sharing-Anwendungen, Proxy-Anonymisierer, Speicher-Anwendungen, schädliche Websites und mehr.
- Analyse von Malware-Bedrohungen und Computern, die mit Bots, Viren und unbekannter Malware infiziert sind (Zero-Day-Angriffe und Malware kann von traditionellen Anti-Virus-Systemen nicht erkannt werden).
- Ausgenutzte Schwachstellen bei Servern und Computern im Unternehmen, die auf mögliche Angriffe hinweisen können.
- Geschäftskritische Daten, die per E-Mail oder über das Internet versendet werden und Ihr Unternehmensnetzwerk verlassen.
- Bandbreitenanalyse, die die Anwendungen und besuchten Websites identifiziert, die die meiste Bandbreite nutzen.

Ergebnis und Bericht mit folgenden Inhalten:

- Informationen zu Computern, die mit Malware infiziert sind.
- Informationen zu risikoreichen Web-Anwendungen und Websites.
- Informationen zu ausgenutzten Schwachstellen und Angriffen auf Ihr Netzwerk.
- Informationen zu Datenverlusten.
- Empfehlungen zum Schutz Ihres Netzwerks vor Sicherheitsrisiken.

Ihr Ansprechpartner:

CGM IT Design und Service
André Schulze
T +49 (0) 7355 799-644
andre.schulze@cgm.com

cgm.com/de