SUEBO Informatik AG

Besser sicher drahtlos
als unsicher und ratlos

Wi-Fi Security

Cyberangriffe stellen die öffentliche Verwaltung, Organisationen und Unternehmen vor eine ernsthafte Herausforderung

Praktisch jedes moderne Unternehmen ist betroffen. Die drahtlose Technik bietet uns viel Flexibilität, doch sie birgt auch erhebliche Risiken.

RISIKOSITUATION:

Bei allen Vorteilen, welche diese Technologie mit sich bringt, besteht das grosse Problem, dass Angreifer keinen physikalischen Zugang zu einem Netzwerk benötigen, sondern Ihre Organisation unauffällig aus der Ferne angreifen können.

ANGRIFFSTECKNIKEN:

Es gibt zahlreiche verschiedene Arten von Angriffstechniken: Angriffe auf die Verschlüsselung, Rouge-AP, Man-in-the-Middle, DoS, MAC-Spoofing, Evil Twin, Fragmentierung, Karma Attacken, Packet Injection, Deauthentication, Beacon-Flooding, Wi-Fi Phishing, AP Spoofing, Wi-Fi Jamming, Bluetooth-Attacken, etc. Fast täglich gibt es neue Werkzeuge, um solche Angriffe mit wenig Wissen und geringem Aufwand durchführen zu können.

GEGENMASSNAHMEN:

Die Experten der SUEBO Informatik AG kennen die effizientesten Gegenmassnahmen um Sie optimal beraten und vor Angriffen schützen zu können.

Wir sind Ihr Partner für Cybersicherheit und unterstützen Sie bei der Vorbereitung zukünftiger Herausforderungen in diesem Umfeld.

SUEBO Informatik AG Sinserstrasse 67, CH-6330 Cham security@suebo.ch www.suebo.ch

SUEBO Informatik AG

Sind Sie bereit für die Zukunft?

"Secure Wi-Fi is like a seatbelt - it protects you from harm and you don't notice it's there until you need it."

Darren Kitchen,
Technologie-Experte
und CEO von Hak5 LLC

Denken Sie daran: Kriminelle arbeiten international. Cyberangriffe bedrohen unsere kritische Infrastruktur, öffentlichen Verwaltungen, Organisationen und Unternehmen auf aller Welt und jeden Tag.
Es ist wichtiger denn je, Ihre IT-Sicherheit zu überprüfen.

RISIKOBASIERTE GEGENMASSNAHMEN

WLAN-Netzwerke sind anfälliger für Sicherheitsrisiken wie Datenlecks und unbefugten Zugriff, da sie drahtlos sind und aus der Distanz aus zugänglich bzw. angreifbar sind. Wir zeigen Ihnen wie Sie effektive Gegenmassnahmen, für Ihre Institution identifizieren, planen und umsetzen können. Hier auszugsweise einige Beispiele aus der Praxis:

- Einführen eines professionellen Passwortmanagements und Passwortrichtlinien
- Verwendung sicheren Verschlüsselungsstandards in Kombination mit Virtual Private Networks (VPN)
- Einführung von Zwei-Faktor-Authentifizierung
- Patch- und Updatemanagement zur effizienten Aktualisierung Ihrer Firmware und Gerätetreibern
- Verwendung von Intrusion Detection Systemen und WLAN-Monitoring-Tools zur Erkennung und Abwehr von Angriffen
- Konfigurationsoptimierungen z.B. Deaktivierung nicht notwendiger Dienste
- Netzwerksegmentierung und Einschränkung von Remote-Zugriffen
- Schulung der Benutzer und IT-Fachkräften

Es ist wichtig zu beachten, dass die Umsetzung einer einzelnen Massnahme nicht ausreichend ist, um Ihr Netzwerk vollständig zu schützen. Stattdessen sollte risikobasierend eine Kombination verschiedener Massnahmen umgesetzt werden, um realistische Risiken, wirtschaftlich zu minimieren. Die Umsetzung dieser Massnahmen sollte zudem kontinuierlich auf ihre Wirksamkeit geprüft werden. Wir unterstützen Sie gerne bei Ihrer individuellen Umsetzung.

IHRE VORTEILE:

Sie profitieren mit Ihrer Umsetzung von Gegenmassnahmen gleich mehrfach:

- **«Quick-Wins» identifizieren (geringer Aufwand / grosser Mehrwert)**
- **Einschätzung bereits getroffener Sicherheitsmassnahmen**
- **Identifikation möglicher Schwachstellen**
- **Definieren gezielter Sicherheitsmassnahmen zur Schliessung von Lücken**
- **Sensibilisierung der Beteiligten für Gefährdungen**
- **Umfassendes Branchen-Wissen unserer IT-Spezialisten**

SUEBO Informatik AG Sinserstrasse 67, CH-6330 Cham security@suebo.ch www.suebo.ch