IT Notfallskarte security

https://magsecurity.at

Ruhe bewahren & Vorfall melden

Ihre IT Notfallsnummer

+43 1 406 00 97 0

MAG Mental Acrobatics Group,1030 Wien, Arsenal 16 Top 66

Montag bis Donnerstag von 09.00 Uhr bis 16.00 Uhr, Freitag von 09.00 Uhr bis 12.00 Uhr

Schritt 1 - Netzwerktrennung

Trennen Sie die physikalische Netzwerkverbindung, entweder das **Netzwerkkabel entfernen** oder **WLAN sofort deaktivieren**.

Schritt 2 - Systemabschaltung

Schalten Sie das betroffene System (PC, Server, Switch, Modem, Router, etc.) ab und **ziehen Sie das Stromkabel** ab. Sollte Ihr System nicht mehr reagieren z.B. herunterfahren des Computers, so ziehen Sie in letzter Konsequenz den Stromstecker.

Versuchen Sie keine Selbstreparaturen
z.B. mit Software aus dem Internet,
dies verursacht meist noch mehr Ärger !!!

Schritt 3 - Meldung

Melden Sie nun Ihrem Vorgesetzten oder Ihrer IT Abteilung, falls vorhanden, den Sicherheitsvorfall. Ist niemand erreichbar, so können Sie auch direkt das Team der MAG kontaktieren.

Was ist zu melden ?

- **Ihr Namen, Firma, Abteilung**
  Rückrufnummer (event. Mobile Erreichbarkeiten)
- **Welches System ist betroffen und seit wann?**
  (eventuell interne Nummer, Seriennummer, ...)
- **Verhalten des Systems**
  Was ist passiert, was wurde bereits getätigt? (Schritte 1-2)
- **Wie ist es passiert?**
  z.B. öffnen eines Email Anhangs, beim Surfen im Internet, Anschluss eines externen Gerätes (USB, CD, DVD, ...) oder z.B. bei der Installation einer Software, ...

Keine Angst vor Meldungen
es gibt keine Konsequenzen
sofern es nicht illegale Tätigkeiten betrifft

Schritt 4 - Anweisungen abwarten

Schalten Sie das betroffene System nicht wieder ein oder ähnliches, warten Sie die Anweisungen der IT bzw. Ihres Vorgesetzten ab. Ruhe bewahren, nun sind die Profis am Werk.

Hinweise zum Selbstschutz

Emails - Unbekanntes nie öffnen

Heute werden maßgeschneiderte Emails versendet, um entweder an Daten zu gelangen z.B. Passwörter, Bankdaten, oder ähnliche Daten (Phishing) oder aber um Ihr System zu infizieren (z.B. Ransomware & Trojaner wie Emotet). **Öffnen Sie niemals Anhänge von unbekannten Absendern** (z.B. seltsame Bewerbungen mit ZIP Dateien, ...), aber auch **Anhänge von vermeintliche Lieferanten, Partnern und Freunden**. Geben Sie niemals Bankdaten nach Aufforderung ein (z.B. Bank verlangt Änderungen des Accounts, oder ähnliches). **Klicken Sie keine Grafiken und Links in Emails an** mit z.B. Gutscheinen, Mahnungen, Rechtsanwaltsdrohungen oder ähnliche Dinge. Lieber einmal mehr nachfragen und löschen, als ... wenn es wichtig war wird sich der Ansprechpartner nochmals melden, und reagieren Sie nicht auf irgendwelche seltsame Androhungen (auch nicht Klagsdrohungen).

Software - nur freigegebenes installieren

In fast allen Unternehmen darf nur von der Firma freigegebene und geprüfte Software installiert und verwendet werden, dies gilt auch für etwaige „Reparatur Tools", Optimierungssoftware inkl. etwaige Cleaner Software und vermeintliche „ich mache den PC schnelle" Software. Dies stellt oftmals ein herrliches Einfallstor für Schadsoftware dar, selbst von namhaften Seiten die „vertrauenswürdig" scheinen. Wenn Sie etwas benötigen, so hilft Ihnen Ihre IT oder das MAG Team weiter.

Hardware - keine Geschenke anstecken

Es klingt seltsam ist aber so. Wenn Sie z.B. Mäuse, Tastaturen, USB Sticks, USB Geräte aller Art (Taschenlampen, Ladegeräte, ...) oder ähnliches erhalten, dürfen diese nicht verwendet werden, bzw. erst nach Prüfung durch die Sicherheitsprofis. Oftmals enthalten scheinbar harmlose Geschenke z.B. Keylogger, die all Ihre Eingaben (auch Passwörter) weiterleiten. Dies kann selbst die besten Sichertools nicht verhindern, denn dies wird aktiv durch Sie getätigt. Nur geprüfte Hardware darf verwendet werden.

Bei Unsicherheiten besser fragen!
Lieber einmal mehr fragen, fragen ist kostenlos!

Der Ausdruck dieses Dokumentes unterliegt keinem Änderungsdienst.