CYBERBELT©
IHR INTERNET-SICHERHEITSGURT

Ein Interview zur ZTP-Dienstleistung

CYBERBELT©
IHR INTERNET-SICHERHEITSGURT

ZT DI Dr.tech Wolfgang Prentner
CEO . IT-Ziviltechniker . Informatiker
ZTP.digital ZT-GmbH . Prüfstelle für Digitale Sicherheit
+43 (0) 1 532 46 86-0 . info@cyberbelt.net . www.cyberbelt.net

Was sind die häufigsten Bedrohungsszenarien für Unternehmen?

Cyber-Angriffe in Form von Malware sind weltweit verbreitet. Die Malware „Emotet“ beispielsweise, verbreitet sich häufig über Spam- bzw. Phishing-Mails. Dabei werden Fake-E-Mails - die angeblich von Großunternehmen stammen – massenweise mit schadhaften Anhängen (z.B. Dokumente, wie eine Rechnung mit korrupten Makros) versendet. Nachdem sich die Schadsoftware erfolgreich eingeschleust hat, verbreitet sie sich über das lokale Netz. Mit Ransomware kann man sich über E-Mails infizieren, aber auch über Schwachstellen im Browser, Betriebssystem oder in Programmen – dies kann zu fatalen Folgen führen (Beispiel: Ausfälle in der Produktion). Durch Identitätsdiebstahl gelingt es Cyber-Kriminellen mithilfe von Social-Engineering-Methoden, Schadsoftware oder durch Daten-Leaks an personenbezogene Daten heranzukommen, um sie für kriminelle Zwecke zu verwenden.

Wie kann man sich schützen?

Cyber-Angriffe haben viele Gesichter, demnach gibt es unterschiedliche Methoden um sich vor dieser noch unterschätzten Bedrohung zu schützen.
Nach dem Motto „Vorsicht ist besser als Nachsicht“ empfehle ich:

- Eine wirkungsvolle Maßnahme ist es ein ganzheitliches Informationssicherheitsmanagementsystem umzusetzen, um die Basis-Anforderungen festzulegen.
- Schulen Sie Ihre Mitarbeiter ein! Mithilfe der Security-Awareness-Schulung stärken Sie die digitale Eigenverantwortung.
- Backups
- Antivirensoftware
- Patchmanagement
- Netzwerksegmentierung
- Firewalling
- E-Mail-Filter
- Web-Content-Filter
- u.v.m.

Was kann man tun - wenn die Bedrohung bereits akut ist?

Ist der Bedarfsfall eingetreten, ist schnelles Handeln wesentlich. Am besten ist es, wenn Sie einen IT-Sicherheits-Experten konsultieren - wie z.B. ZTP.digital - Die Prüfstelle für Digitale Sicherheit. Bei Notfällen handeln wir sofort um den Schaden möglichst gering zu halten bzw. zu beseitigen. Im Falle von Ransomware empfehle ich hier ganz klar: Ignorieren bzw. die Fake-Rechnung nicht bezahlen. Eine einfache Möglichkeit um die Ausbrei-tung der Schadsoftware innerhalb des lokalen Netzes zu verhindern, ist es eine Spezial-Software einzusetzen oder im Notfall das System herunterzufahren.

„Ist der Bedarfsfall eingetreten, ist schnelles Handeln wesentlich.“

ZTP Eine Dienstleistung der ZTP.digital ZT-GmbH
www.**ztp.digital**

Was ist der CYBERBELT©-Schutz - den Sie anbieten?

Mithilfe des CYBERBELTs werden Ihnen bis zu 52 Schwachstellenberichte pro Jahr (ein Bericht pro Woche) über den Gesundheitszustand Ihrer Systeme von ZTP.digital geliefert. Damit erkennen Sie frühzeitig Gefahren für Ihr Unternehmen und setzen so die richtigen Schutzmaßnahmen auf Basis unserer Prüfberichte um. Mit dem CYBERBELT garantiert ZTP.digital Ihnen Cyber-Sicherheit und Datenschutz mit einem staatlich aner-kannten Cyber-Sicherheitszertifikat auf Basis der aktuellen Gesetze, Standards und Richtlinien.

Informationen zum CYBERBELT©

CYBERBELT© - Ihr Internet-Sicherheitsgurt

Dienstleistungen

- Sicherheits-Audit
- Pentesting
- Social Hacking - Red Team Operations
- Code-Analysen

Kontaktdaten
https://cyberbelt.net
info@cyberbelt.net

CYBERBELT©
Promo-Video

CYBERBELT©
Informations-Video

CYBERBELT©
Website

Für weitere Informationen zum CYBERBELT© - Ihrem Internet-Sicherheitsgurt - besuchen Sie unsere Website www.**cyberbelt.net**