IT-Sicherheit

Achtung Ransomware!

In letzter Zeit häufen sich Vorfälle, in welchen mittels sogenannter "Ransomware" Daten am Rechner und auf Netzlaufwerken verschlüsselt werden und Lösegeld für die Entschlüsselung verlangt wird. Im Prinzip gelten hier die gleichen Vorsichtsmaßnahmen wie beim herkömmlichen Phishing, nur dass nicht das Abgreifen von Zugangsdaten, sondern der Verlust von Dokumenten und anderen Daten das vorrangige Ziel ist.
Tipps zur Vermeidung von Ramsomware

Computersicherheit ist ein wichtiges Thema, nicht nur für Server sondern auch für Arbeitsplätze.

Unsere Aufgabe sehen wir darin, Angriffen gegen die Sicherheit (Hackerattacken, Virenverseuchung etc.) entgegenzuwirken. Ebenso bieten wir Hilfe nach einem Hackerangriff oder einem Virenbefall an.

Weiters möchten wir unsere Erfahrungen und den Gebrauch von geeigneten Gegenmaßnahmen hier publizieren. Der ZID bietet auch umfangreiche Hilfe in Form von Plattform Unterstützung für Server und Arbeitsplätze an.

Durch das immer schnellere Bekanntwerden von Sicherheitslücken, welche die Hacker ausnutzen, ist ein möglichst schnelles Installieren von Patches notwendig. Daher sollten die bei allen gängigen Plattformen vorhandenen Update-Dienste regelmäßig benutzt werden.

Der beste Beitrag zur Sicherheit ist sicherlich die Prävention - wenn ein Rechner einmal gehackt ist, bedeutet dies meistens eine Neuinstallation. Um das zu vermeiden, hier ein paar Tipps:

- Keine offenen Dienste ohne Passwörter oder default Passwörter, nur die Dienste auf dem Rechner installieren, die wirklich benötigt werden.
- Keine unsicheren Logins per Telnet, sondern SSH verwenden. Wir empfehlen frei erhältliche Software (SSH-Clients wie puTTY, WinSCP oder Virenscanner wie Avira und Avast in der jeweiligen Free-Variante, etc.), vgl. z. B. Campus-Software-Angebot.
- Diese Dienste immer auf dem neuesten Versionsstand halten, bei Windows Clients: immer Virenscanner und auch Trojanerscannner installieren (am besten mit Internetupdatefunktion).
- Bei Neuinstallation Checksummen aller Programme auf ein externes Medium speichern (bei Änderungen diese Daten auf dem externen Medium aktualisieren).
- Logfiles auch auf einen externen Rechner speichern, da Hacker auf dem angegriffenen Rechner ihre Spuren verwischen.
