Wie kann ich mich vor Ransomware schützen?

1. **Backups anlegen (3-2-1 Regel)**
   Alt aber bewährt! Legen Sie in regelmäßigen Abständen Backups Ihrer Daten an. Beachten Sie, dass Sie das Speichermedium vom Rechner abkoppeln, sonst kann es ebenfalls Opfer der Verschlüsselung werden.

   netvision Lösung: Managed Backup

2. **Updates und Patches installieren**
   Jede installierte Software, vom Betriebssystem über Büro-Anwendungen bis hin zu Laufzeitumgebungen (Flash Player), birgt potenzielle Sicherheitslücken. Diese werden von Malware-Programmierern ausgenutzt. Um diese potenziellen Lücken zu schließen, sollten Sie alle Programme regelmäßig updaten.

   netvision Lösung: Managed Security - Wartung und Absicherung

3. **Unsichere Webseiten vermeiden**
   Dies gilt generell und ist bekannt. Die meisten Dienstleistungen im Internet befinden sich auf sicheren Seiten. Sollte sich die Nutzung einer unsicheren Seite dennoch nicht vermeiden lassen, sollte ein Virenscanner und Ransomware-Schutz aktiviert sein.

   Sichere Webseiten können als Lesezeichen gespeichert und bevorzugt genutzt werden. Aber Vorsicht: Links in Phishing-Mails führen oft zu betrügerischen Webseiten, die vom Original optisch nicht zu unterscheiden sind. Achten Sie vor dem Klick auf Buttons erst einmal auf die Web-Adresse, die in der linken unteren Ecke des Browsers oder Mailclients angezeigt wird, wenn Sie die Maus über den Link führen. Sehen Sie eine URL, die nichts mit dem Namen der besuchten Webseite oder des Webseiten-Betreibers zu tun hat, verzichten Sie besser auf den Klick.

   netvision Lösung: Managed Security - Wartung und Absicherung sowie Messaging-Gateways und Internet-Gateways

4. **Öffnen Sie nur von bekannten Absendern E-Mails und E-Mail-Anhänge**
   E-Mails unbekannter Absender gelangen immer wieder unerkannt in E-Mail-Postfächer. Verringern Sie die Gefahr, Opfer von Ransomware zu werden, indem Sie nichts öffnen, was Sie nicht kennen oder Ihnen merkwürdig erscheint. Selbst wenn Sie den Absender kennen, lassen Sie sich nicht täuschen! Überprüfen Sie den Absender noch einmal zur Sicherheit. Folgende Dateitypen sollten Sie grundsätzlich aufmerksam werden lassen: Microsoft Office Dokumente, wie doc, docx, docm, xls, xlsx, xlm, usw., .exe, .bat, .zip, .reg sowie .vbs. Im Zweifel versichern Sie sich besser bei dem bekannten Absender, ob er Ihnen tatsächlich eine Mail geschickt hat oder fragen Sie bei Ihrem IT-Betreuer nach.

   netvision Lösung: Managed Security - Wartung und Absicherung sowie Messaging-Gateways und Internet-Gateways

5. **Software für den Schutz vor Ransomware installieren**
   Installieren Sie eine aktuelle Schutz-Software, zusätzlich zu den regelmäßigen Backups und dem aufmerksamen Umgang mit dem Internet. Dies sichert Sie noch besser gegen Ransomware, wie WannaCry, ab!

   netvision Lösung: Managed Antivirus / Predictive Machine Learning und Weitere

Bei weiteren Fragen stehen wir Ihnen jederzeit gerne zur Verfügung!

Ihr netvision-Team

netvision Datengechnik GmbH u. Co. KG

In der Wanne 53, 89075 Ulm
Telefon: +49 (0) 731 550 493 0
Telefax: +49 (0) 731 550 493 29
E-Mail: Info netvision
Website: www.net-vision.de

Geschäftsführer: Christian Walter
Registergericht Ulm HRA 2721