Das Bewusstsein erhöhen für (Internet-Gefahren)

19.05.2016

Auf einen Blick

economiesuisse engagiert sich in der Sensibilisierung für «Ransomware». Wie schützt man sich als KMU oder Privatperson vor den Erpressungs-Trojanern? Laden Sie sich das Merkblatt des Bundes herunter.

In den letzten Monaten hat sich die Zahl der Opfer von Ransomware in der Schweiz drastisch erhöht. Unlängst wurden nicht mehr nur Privatanwender Ziel von Angriffen mit Ransomware, sondern vermehrt auch kleine und mittlere Unternehmen (KMU). Während Privatpersonen nicht mehr auf ihre persönlichen Daten zugreifen können, hat Ransomware bei Unternehmen meist gravierende Auswirkungen. Verträge, Kunden- oder Buchhaltungsdaten und weitere unternehmenskritische Daten werden verschlüsselt und somit unbrauchbar.

Ein Vorfall mit Ransomware (auch «Sperrtrojaner» oder «Erpressungstrojaner» genannt) läuft in der Regel so ab:

- Typischerweise verbreitet sich Ransomware durch das Öffnen schädlicher E-Mail-Anhänge oder über gehackte Websites.
- Einmal infiziert, werden Dateien auf dem Computer verschlüsselt. Das können auch Dateien auf verbundenen Netzlaufwerken (Network shares) und Speichermedien sein (zum Beispiel USB-Sticks).
- Verschlüsselte Dateien sind für das Opfer nicht mehr zugänglich.
- Nun zeigt die Ransomware dem Opfer einen «Sperrbildschirm» an. Er fordert das Opfer auf, eine bestimmte Geldsumme in Form einer Internetwährung (beispielsweise Bitcoins) zu bezahlen. Als Gegenzug geben die Angreifer die verschlüsselten Dateien wieder frei (Erpressung).

economiesuisse engagiert sich in der Sensbilisierung für Ransomware. Wie kann man sich als KMU, aber auch als Privatperson vor Ransomware schützen? Und was tun, wenn es doch zu einer Attacke gekommen ist? Das Merkblatt «Ransomware» der Melde- und Analysestelle Informationssicherung des Bundes (Melani) liefert Ihnen die Antworten. Besuchen Sie auch die Website von Melani für mehr Informationen über Ransomware.