Sie sind das Ziel

Benutzernamen & Passwörter

Haben sie einmal Zugang erlangt, können Cyberkriminelle auf Ihrem Computer Programme installieren die alle Tastendrücke mitschreiben, inklusive Ihren Benutzernamen und Passwörtern. Mit diesen Informationen meldet man sich dann bei Ihren Online-Zugängen an, darunter:

- Ihre Bank- oder Finanzzugänge, um Geld zu stehlen.
- Ihr iCloud, Google Drive, oder Dropbox Zugang, was Zugriff auf all Ihre dort gespeicherten Daten erlaubt.
- Ihr Amazon, eBay oder sonstiger Online Shopping Zugang womit Waren in Ihrem Namen und auf Ihre Rechnung gekauft werden.
- Ihre Packstation Zugang, um gestohlene Güter in Ihrem Namen zu versenden.

Sammlung von E-Mail Konten

Haben sie einmal Zugang erlangt, können Cyberkriminelle Ihre E-Mails auswerten um Informationen zu gewinnen welche sie an Dritte verkaufen können, darunter z.B.:

- Alle Namen, E-Mail Adressen und Telefonnummern Ihrer Kontaktliste.
- Ihre gesamten beruflichen oder private E-Mail Kommunikation.

Virtuelle Güter

Haben sie einmal Zugang erlangt, können Cyberkriminelle von Ihrem Computer virtuelle Güter stehlen oder kopieren und dann verkaufen, darunter:

- Computerspiel-Charaktere, -Waren oder -Zahlungsmittel.
- Softwarelizenzen, Betriebssystem-Lizenzschlüssel oder Spielelizenzen.

Bot-Netze

Haben Cyberkriminelle einmal Zugang erlangt, kann Ihr Computer Teil eines grossen Netzwerks kompromittierter Computer werden, die von Kriminellen kontrolliert werden. Dieses Netzwerk, Bot-Netz genannt, kann dann für z.B. die folgenden Aktivitäten genutzt werden:

- Spam E-Mail an Millionen Benutzer zu versenden
- Denial of Service Angriffe durchzuführen, die Webseiten und Webdienste lahmlegen.

Indentitätsdiebstahl

Haben Cyberkriminelle einmal Zugang erlangt, können sie Ihre Online-Indentitäten stehlen um damit selbst Betrug zu begehen oder sie weiterzuverkaufen, darunter z.B.:

- Ihr Facebook, Twitter, Xing, oder LinkediIn Zugang.
- Ihre E-Mail Zugänge.
- Ihre Skype oder sonstige Chat-Zugänge.

Webserver

Haben Cyberkriminelle einmal einen Zugang erlangt, können sie Ihren Computer in einen Webserver verwandeln, den sie z.B. für Folgendes nutzen:

- Bereistellung von Phishing Webseiten, um Nutzernamen und Passwörter Dritter zu stehlen.
- Bereistellung von Angriffswerkzeugen welche die Computer Dritter kompromittieren.
- Ablage und Verteilung von Kinderpornografie, raubkopierten Videos oder gestohlener Musik.

Finanzdaten

Haben Cyberkriminelle einmal einen Zugang erlangt, können sie Ihren Computer nach wertvollen Invormationen absuchen, darunter z.B.:

- Ihre Kreditkarteninformationen
- Ihre Steuerdaten und Steuererklärungen.
- Ihre Investment- und Sparpläne.

Erpressung

Haben Cyberkriminelle einmal einen Zugang erlangt, können sie diesen übernehmen und Geld fordern für:

- Die Vernichtung oder Nicht-Veröffentlichung von Bildern, die sie heimlich mit der eingebauten Kamera aufgenommen haben.
- Die Entschlüsselung aller Daten, die mit einem nur den Kriminellen bekannten Schlüssel verschlüsselt wurden.
- Die nicht- Veröffentlichung der von Ihnen besuchten Webseiten, über die die Kriminellen Protokoll führen.

Security Awareness Training

Bei Ihnen vor Ort
In unseren modernen Schulräumen in Olten
Pro Gruppe ca. 1 Stunde

Tagespauschale Fr. 2250.- (max. 4 Gruppen)
Schon mehrfach erfolgreich durchgeführt mit besten Feedbacks.
Referenzen auf Anfrage

itee.ch

Das schwächste Glied in der Kette bestimmt den Level Ihrer Security!