ontexx • IT-Support
Inh. Stefan Schmidt
Am Kalkofen 5 | 67346 Speyer |
Deutschland
Tel.:+49 (6232) • 8 77 22 72
info@ontexx.de
www.ontexx.de

Sicherheit im Netzwerk – ein kleiner Ratgeber für unsere Kunden

Wie kann ein IT-System von Schadsoftware befallen werden?

- Bekannte **Sicherheitslücken in verwendeter Software** bieten professionellen Hackern aber auch Laien die Möglichkeiten, Schadsoftware auf einem Rechner einzuschleusen.
- Der am meisten verwendete Weg, Schadsoftware zu verteilen und auf Rechnern zu installieren, ist die massenhafte Versendung von **E-Mails mit infizierten Anhängen**. Auch ein Link auf einer Internetseite oder in einer E-Mail kann direkt zu einer Schadsoftware führen.

Welche Maßnahmen können getroffen werden, um sich vor Schadsoftware oder unberechtigtem Zugriff auf Ihr IT-System zu schützen?

- Das Betriebssystem durch Updates auf aktuellem Stand halten
  - Bekannte Sicherheitslücken werden geschlossen
  - Weitere Sicherheitssysteme werden installiert
- Updates von eingesetzter Software und Plugins regelmäßig durchführen
  - Bekannte Sicherheitslücken werden geschlossen
  - Zugriffe von Hackern werden verhindert
- Firmware von Hardware regelmäßig aktualisieren
  - Sicherheitslücken werden geschlossen
  - Die Leistung der Geräte wird verbessert
- Backups von Daten regelmäßig durchführen
  - Im Schadensfall kann man auf die gesicherten Daten zurückgreifen, der Datenverlust bleibt gering
  - Bei einer Neuinstallation nach einem Hackerangriff können die wichtigsten Daten schnell wieder auf den Rechner zurückgespielt werden
- Der Einsatz einer Firewall und eines Antivirenprogramms mit Echtzeitschutz ist zwingend erforderlich
  - Schadsoftware kann durch den Echtzeitschutz sofort erkannt und entfernt werden, noch bevor es zu Verlusten von Daten kommt
  - Eine Firewall schließt Zugriffsmöglichkeiten in IT-Systemen, die von Hackern verwendet werden
  - Regelmäßige Virenscans des gesamten PCs können Schadsoftware entdecken und verhindern Datenverlust oder -Spionage

ontexx • IT-Support
Inh. Stefan Schmidt
Am Kalkofen 5 | 67346 Speyer |
Deutschland
Tel.:+49 (6232) • 8 77 22 72
info@ontexx.de
www.ontexx.de

- Berechtigungen des Benutzeraccounts einschränken
  - Bei administrativen Berechtigungen hätte eine Schadsoftware sofort volle Zugriffsberechtigungen auf das gesamte System
  - Benutzer mit eingeschränkten Rechten können keine Schadsoftware installieren, ein Administrator ist dafür nötig

- Internetzugangsdaten vom Provider oder Standarddaten in Routern ändern
  - Allgemein bekannte Standardzugangsdaten von Internetprovidern oder auf Hardwaregeräten (z.B. Routern) können durch Fremde genutzt werden, um sich Zugang auf diese Systeme zu verschaffen

- Wireless LAN (WLAN) absichern
  - WLAN nur bei Nutzung aktivieren
  - Verschlüsselung zur Datenübertragung aktivieren
  - Passwort zur Verbindung nutzen
  - SSID (Name des WLAN) nicht aussenden (nicht sichtbar)
  - SSID Bezeichnung ohne Bezug auf Firma oder Ort wählen

- MAC-Adressfilterung nutzen
  - Nur eingetragene Geräte (Identifikation über die MAC Adresse) erhalten Zugang zum Netzwerk
  - Fremde, unbekannte Geräte werden nicht zugelassen

- Vergabe von sicheren Passwörtern

Was ist ein sicheres Passwort?
Ein sicheres Passwort kennt nur der Anwender selbst und sonst kein anderer. Es ist nirgendwo aufgeschrieben, enthält alle vier Zeichentypen kombiniert (Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen) und sollte im Idealfall mindestens zwölf Zeichen lang sein.

Aus der Praxis ist bekannt, dass Kennwörter gerne auf einem Zettel unter der Tastatur, in der obersten Schublade oder direkt am Monitor kleben, so kann man sich ein Passwort auch gleich sparen!

- Überlegtes Handeln – Die Verantwortung liegt beim Anwender

Überlegtes Handeln beim Öffnen von Dateianhängen und Anklicken von Links in E-Mails oder auf Internetseiten sind entscheidend, ob eine Schadsoftware unerkannt Zugriff auf den Rechner erhält oder nicht. Man sollte immer zuerst die Sicherheit einer Quelle (Überprüfung der Seriosität von E-Mails und Internetseiten) bewerten, bevor man dieser vertraut.
Überlegtes Handeln bietet den besten Schutz gegen jegliche Art von Angriffen.

! Achtung !
Updates, Firewall und Antivirenprogramme können durch unüberlegtes Handeln für jede Schadsoftware einfach umgangen werden, wenn man z.B. durch Anklicken eines Links oder Öffnen einer unbekannten Datei dem Schädling direkt den Zugang gewährt!
So wird meistens vom Anwender selbst unbewusst der Schadsoftware die Erlaubnis erteilt, sich auf dem Rechner zu installieren.

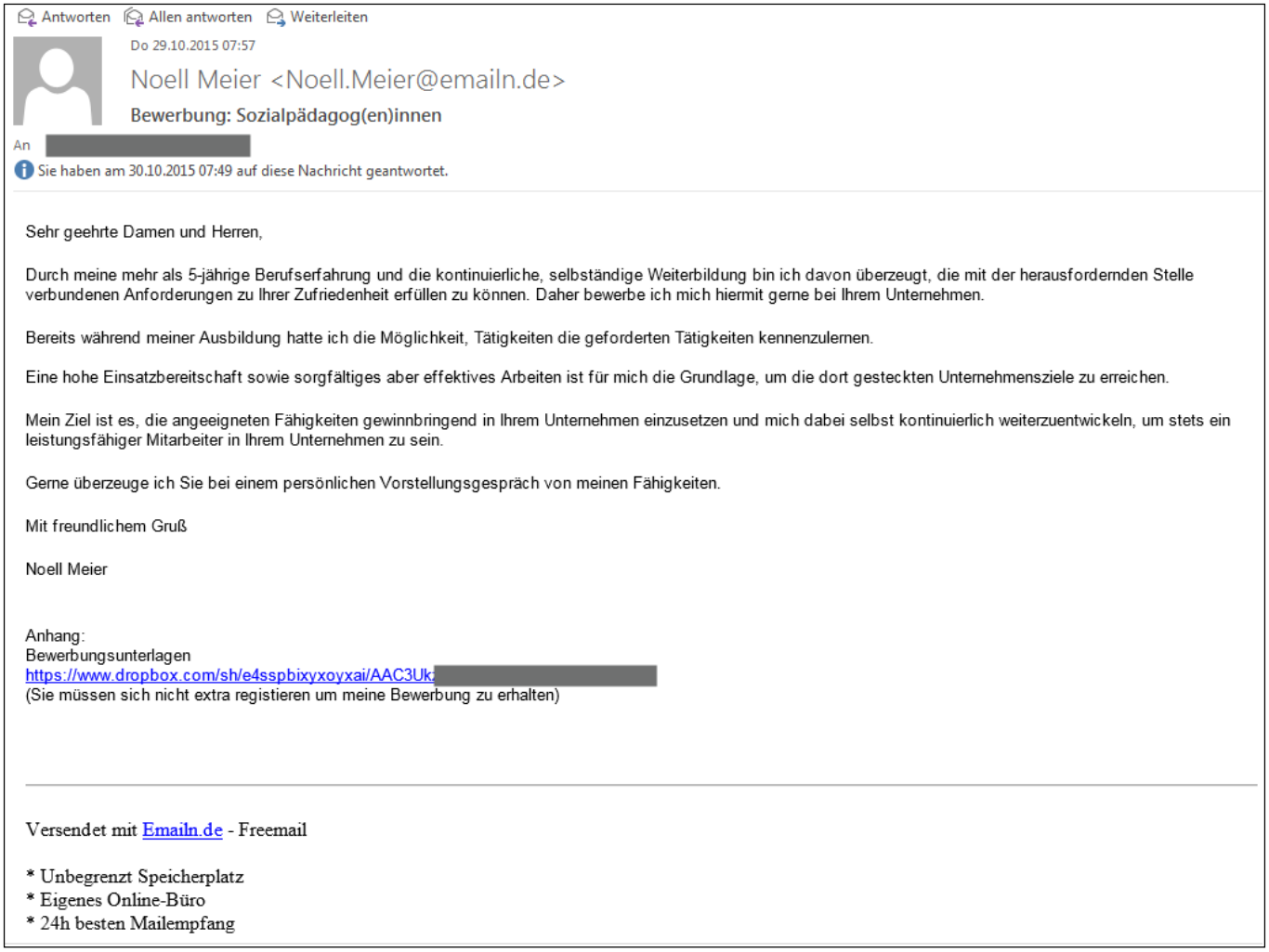
ontexx • IT-Support
Inh. Stefan Schmidt
Am Kalkofen 5 | 67346 Speyer | Deutschland
Tel.:+49 (6232) • 8 77 22 72
info@ontexx.de
www.ontexx.de

Eine weitverbreitete Meinung, dass Linux und Apple Systeme nicht von Schadsoftware betroffen sind, stimmt nicht. Für alle Systeme sind schadhafte Programme im Umlauf, die auch Linux und Apple Rechner infizieren.
Da die meisten IT-Systeme jedoch Microsoft-Systeme sind, gibt es auch für diese Systeme häufiger Angriffe, potentiell gefährdet sind aber alle Systeme.

Beispiele aus der Praxis

1. Bewerbungsmail mit schadhafter Software

Die Personalabteilung eines Unternehmens erhielt nach einer Stellenausschreibung folgende E-Mail:



Antworten Allen antworten Weiterleiten

Do 29.10.2015 07:57

Noell Meier <Noell.Meier@emailn.de>

Bewerbung: Sozialpädagog(en)innen

An [redacted]

Sie haben am 30.10.2015 07:49 auf diese Nachricht geantwortet.

Sehr geehrte Damen und Herren,

Durch meine mehr als 5-jährige Berufserfahrung und die kontinuierliche, selbständige Weiterbildung bin ich davon überzeugt, die mit der herausfordernden Stelle verbundenen Anforderungen zu Ihrer Zufriedenheit erfüllen zu können. Daher bewerbe ich mich hiermit gerne bei Ihrem Unternehmen.

Bereits während meiner Ausbildung hatte ich die Möglichkeit, Tätigkeiten die geforderten Tätigkeiten kennenzulernen.

Eine hohe Einsatzbereitschaft sowie sorgfältiges aber effektives Arbeiten ist für mich die Grundlage, um die dort gesteckten Unternehmensziele zu erreichen.

Mein Ziel ist es, die angeeigneten Fähigkeiten gewinnbringend in Ihrem Unternehmen einzusetzen und mich dabei selbst kontinuierlich weiterzuentwickeln, um stets ein leistungsfähiger Mitarbeiter in Ihrem Unternehmen zu sein.

Gerne überzeuge ich Sie bei einem persönlichen Vorstellungsgespräch von meinen Fähigkeiten.

Mit freundlichem Gruß

Noell Meier

Anhang:
Bewerbungsunterlagen
https://www.dropbox.com/sh/e4sspbixyxoyxai/AAC3Uk[redacted]
(Sie müssen sich nicht extra registieren um meine Bewerbung zu erhalten)

Versendet mit Emailn.de - Freemail

* Unbegrenzt Speicherplatz
* Eigenes Online-Büro
* 24h besten Mailempfang

Nachdem sich der verantwortliche Vorgesetzte über den unter der E-Mail angegebenen Link die Bewerbungsunterlagen anschauen wollte, wurde er aufgefordert sich dort anzumelden und bekam dann per E-Mail einen weiteren Link zugesandt, über den er die Anmeldung bestätigen sollte.
Durch die Bestätigung gab er so einer Schadsoftware freien Zugriff auf seinen Rechner.

Trotz Firewall und Antivirusprogramm erlaubte so der Anwender der Software sich zu installieren, was zur Folge hatte, dass alle Word-, Excel- und andere Dokumente verschlüsselt wurden (256 Bit-Verschlüsselung) und der Zugriff für den Anwender nicht mehr möglich war.

ontexx • IT-Support
Inh. Stefan Schmidt
Am Kalkofen 5 | 67346 Speyer |
Deutschland
Tel.:+49 (6232) • 8 77 22 72
info@ontexx.de
www.ontexx.de

Diese Art der Schadsoftware nennt sich „Ransomware“, die Zugriffs- oder Nutzungsverhinderungen von Daten oder des gesamten Computersystems erwirkt.
Durch Überweisung eines Betrages (in diesem Fall 400,- Euro) würden die Daten wieder entschlüsselt werden und so die Verwendung erst wieder für den Anwender möglich.

Es bleibt fraglich, ob auch nach einer Überweisung die Daten wirklich wieder entschlüsselt werden und welche Schadsoftware weiterhin auf dem Rechner zurückbleibt.

Über verschiedene IT-technische Vorkehrungen ist es ohne weiteres auch nicht möglich, den Absender der E-Mail ausfindig zu machen.

Wie hätte man diesen Befall verhindern können?

- **eingeschränktes Benutzerkonto ohne Adminrechte**
  Dieser Befall wäre durch ein eingeschränktes Benutzerkonto (keine Administratorenrechte) verhindert worden, denn ohne ausreichende Berechtigungen hätte sich die Schadsoftware schon gar nicht installieren können.

- **keine Downloads und Installationen von unbekannten Quellen (in diesem Fall Absender)**
  Alle angebotenen Downloads und Aufforderungen zu Installationen von unbekannten Quellen (u.a. Internetadressen, E-Mail Adressen, Links) müssen mit äußerster Vorsicht behandelt werden.
  Der E-Mail Absender (in diesem Fall „Noell.Meier@emailn.de“) ist für den Empfänger nicht bekannt. Dabei darf man „bekannt“ nicht mit „unauffällig“ verwechseln, denn die E-Mail Adresse scheint durch den eingefügten Namen personalisiert zu sein und weckt Vertrauen.
  Zusätzlich sind in einer Bewerbungs-E-Mail gewöhnlich alle Anhänge (u.a. Zeugnisse, Lebenslauf) als PDF-Dateien angehängt und dafür muss keine Software installiert werden.

Weitere Infos zu dieser Schadsoftware finden Sie auf den Internetseiten der Polizei:
http://www.polizei-praevention.de/aktuelles/chimera-ransomware.html

2. Fahrzeugsoftware mit SMS manipuliert

Ein Beispiel aus der KFZ-Industrie zeigte, dass über eine einfache SMS eine Sicherheitslücke in einer Corvette (Chevrolet) überlistet werden konnte und sich Zugang zu verschiedenen Fahrzeugfunktionen verschafft wurde. Neben der Übernahme der Kontrolle über die Scheibenwischanlage konnte auch das Bremssystem manipuliert werden.

Quelle (Internetseite Automobilwoche):
http://www.automobilwoche.de/article/20150812/NACHRICHTEN/308129902/nach-jeep-tesla-und-chevrolet-hacker-legen-per-handy-corvette-bremsen-lahm#.ViCuijaheHs