PRO LAN
COMPUTER GMBH

Security - Ransomware

Wichtige Grundregeln im Umgang mit Ransomware:

Volksbank Mittelhessen
BLZ: 513 900 00 Kto: 849 766 01
IBAN: DE18 5139 0000 0084 9766 01
BIC: VBMHDE5FXXX

Geschäftsführer: Stefan Rupp
Amtsgericht: Friedberg
Handelsregister: HRB 1400
USt.-IdNr.: DE 159 169 598

Inhaltsübersicht

1. Regelmäßige Datensicherung 3
2. Dateianhänge blockieren 3
3. Makros in Office-Programmen deaktivieren 3
4. Seien Sie immer misstrauisch! 3
5. Software aktuell halten 3
6. Arbeiten Sie nur mit Minimal-Berechtigungen 3
7. Aufklären 3
8. Weiterführende Informationen zum Thema Ransomware: 4

Volksbank Mittelhessen
BLZ: 513 900 00 Kto: 849 766 01
IBAN: DE18 5139 0000 0084 9766 01
BIC: VBMHDE5FXXX

Geschäftsführer: Stefan Rupp
Amtsgericht: Friedberg
Handelsregister: HRB 1400
USt.-IdNr.: DE 159 169 598

1. Regelmäßige Datensicherung

Zusätzlich zur täglichen Datensicherung sollte eine weitere Datensicherung auf Offlinemedien stattfinden, da Verschlüsselungstrojaner inzwischen auch Netzwerkspeicher verschlüsseln. Offlinespeicher sind Datensicherungsmedien, die unmittelbar nach der Sicherung offline genommen werden, also vom Netzwerk getrennt werden. Dazu gehören z.B. RDX-Speichermedien oder LTO-Datensicherungsbänder.

2. Dateianhänge blockieren

E-Mails mit Dateianhängen, insbesondere mit Word- oder Excel-Dokumenten, prinzipiell von der Firewall blockieren lassen. Ransomware schleust sich meist durch Dateianhänge an E-Mails in das Netzwerk ein. Warum gesondert auf Word- und Excel-Dokumente achten? Word und Excel bieten praktische Makrofunktionen. Leider werden diese Funktionen häufig dazu genutzt, die Schadsoftware zu aktivieren.

3. Makros in Office-Programmen deaktivieren

Vgl. Punkt 2. Deaktivieren Sie die Makro-Funktionen in Office-Programmen, wenn diese nicht zwingend genutzt werden.

4. Seien Sie immer misstrauisch!

Öffnen Sie nicht wahllos jeden Link und jeden Dateianhang in einer E-Mail, insbesondere nicht wenn Sie den Absender nicht kennen.

5. Software aktuell halten

Halten Sie Ihre Software stets auf dem aktuellen Stand. Insbesondere die Betriebssysteme, Virenschutzprogramme, Firewalls, aber auch Browser, Flash-Player, PDF-Reader. Regelmäßige Updates der Softwarehersteller schließen oft gefährliche Sicherheitslücken in den Programmen.

6. Arbeiten Sie nur mit Minimal-Berechtigungen

Nutzen Sie für die tägliche Arbeit Benutzer mit Minimal-Systemberechtigungen. Diese sind für die tägliche PC-Arbeit in der Regel vollkommen ausreichend.

7. Aufklären

Klären Sie Ihre Mitarbeiter auf! Zeigen Sie Ihnen den „richtigen“ Umgang mit E-Mails.

Volksbank Mittelhessen
BLZ: 513 900 00 Kto: 849 766 01
IBAN: DE18 5139 0000 0084 9766 01
BIC: VBMHDE5FXXX

Geschäftsführer: Stefan Rupp
Amtsgericht: Friedberg
Handelsregister: HRB 1400
USt.-IdNr.: DE 159 169 598

8. Weiterführende Informationen zum Thema Ransomware:

https://www.computerwoche.de/a/fuenf-empfehlungen-fuer-wannacry-opfer,3330745

https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/Ransomware/Ransomware_node.html

http://hessenschau.de/panorama/cyberattacke-trifft-auch-die-bahn-in-hessen,cyber-attacke-frankfurt-100.html

Für weitere Fragen oder Unterstützung bei der Umsetzung der oben genannten Punkte kontaktieren Sie das ProLan-Berater Team unter: **+49 (6034) 9396-0.**

Volksbank Mittelhessen
BLZ: 513 900 00 Kto: 849 766 01
IBAN: DE18 5139 0000 0084 9766 01
BIC: VBMHDE5FXXX

Geschäftsführer: Stefan Rupp
Amtsgericht: Friedberg
Handelsregister: HRB 1400
USt.-IdNr.: DE 159 169 598