DIGITAL SICHER NRW
Kompetenzzentrum für Cybersicherheit in der Wirtschaft

Beauftragt vom
Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen

VON ANGREIFERN LERNEN

Alle Punkte wurden Betroffenen im Rahmen einer Lösegeld-Verhandlung zugespielt, um sich vor Ransomware-Angriffen und anderen Attacken effektiv zu schützen.

1. Administratoren müssen in Browsern im privaten Modus arbeiten.

2. Administratoren ist es untersagt, Passwörter in Browsern zu speichern.

3. Administratoren ist es untersagt, Dateien mit Passwortlisten auf ihren Computern oder gemeinsam genutzten Ressourcen zu speichern und per E-Mail zu versenden.

4. Verdächtige E-Mails dürften nicht geöffnet werden. Wenn sie geöffnet werden sollen, muss dies in geschützter, kontrollierter Umgebung geschehen, z.B. auf Computern ohne Verbindung zum Unternehmensnetzwerk.

   Alle verdächtigen E-Mails mit Links sollten an die IT-Abteilung geschickt werden, damit sie auf einer eigenständigen virtuellen Maschine überprüft werden können.

5. Administratoren arbeiten in virtuellen Maschinen.
   Virtuelle Maschinen müssen in Kryptocontainern untergebracht werden.

6. Firewalls müssen so konfiguriert werden, dass die Computer der Administratoren keinen direkten Zugang zu kritischen Servern haben, die virtuellen Maschinen jedoch schon (Firewall-Regeln und Netzwerkbereiche).

7. Beschränken Sie die Liste der Domänenadministratoren. Das Domänenadministrator-Passwort sollte zwischen Sicherheitsabteilung und Verwaltungsabteilung aufgeteilt werden (das Passwort ist sehr lang).

8. Teilen Sie die Verantwortung so auf, dass verschiedene Administratoren unterschiedliche Rechte haben und verwalten (kleine regelmäßige Aufgaben wie Zurücksetzen von Passwörtern, Anlegen von Benutzern wird weniger restriktiv gehandhabt als tiefergehende und komplexere Projekte).

DIGITAL SICHER NRW
Kompetenzzentrum für Cybersicherheit in der Wirtschaft

Beauftragt vom
Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen

VON ANGREIFERN LERNEN

9 Verwenden Sie ein starkes Antivirusprogramm.

10 Beschränken Sie den Internetzugang auf Servern und Verwaltungscomputern.
Erstellen Sie einen Terminalserver in der DMZ und benutzen Sie die Terminalbrowser-Anwendungen.

11 Verhindern Sie, dass Benutzer Skript-Programmiersprachen (vbs, js und andere) und unbekannte Dateierweiterungen ausführen können.

12 Öffnen Sie Dokumente mit Makros nur von vertrauenswürdigen Benutzern.

13 Deaktivieren Sie den Remote-Start für Powershell.

14 Zwei-Faktor-Authentifizierung (2FA / MFA) für die Netzwerkinfrastruktur einrichten, insb. um Zugriff auf Backups zu schützen.

15 Halten Sie Ihre Software auf dem neuesten Stand (Updates / Patches)!

16 Verstecken Sie offene Ports nach außen.

VON ANGREIFERN LERNEN

17 Verwenden Sie komplexe Passwörter.

18 Blockieren Sie den Zugriff auf den lsass-Prozess (viele Antivirenprogramme/ Security Suits tun dies).

19 Verwenden Sie das Administratorkonto nur, wenn es nötig ist.

20 Schalten Sie den Computer am Ende des Tages aus.

21 Sperren Sie den Computer bei Verlassen des Arbeitsplatzes.