So schützen Sie sich bei Ransomware

Ransomware-Checkliste

Ransomware wie WannaCry stellt eine wachsende globale Bedrohung für Ihre Daten dar: **Folgen Sie dieser Checkliste, um sich bei einem Ransomware-Angriff zu schützen.**

Ransomware ist eine bösartige Art von Malware, die Dateien auf Ihren Computern und Servern verschlüsselt und ein komplettes Netzwerk in wenigen Minuten infizieren kann. Sobald Ihre Dateien verschlüsselt sind, erpressen Cyber-Kriminelle Bitcoin Lösegeld um Ihre Dateien wieder zu entschlüsseln. Der letzte Angriff, genannt WannaCry, infiziert über 200.000 Systeme in über 150 Ländern in wenigen Tagen. Dies ist eine globale Bedrohung und Sie sollten jetzt handeln und die notwendigen Schritte unternehmen um sich zu schützen.

Bestandsverwaltung

- ☐ Liste aller Software, die im gesamten Netzwerk eingesetzt wird
- ☐ Es gibt keine nicht unterstützten Betriebssysteme (Windows XP oder 2003), die im Netzwerk laufen
- ☐ Keine Verwendung nicht vertrauenswürdiger Software
- ☐ Es sind keine unbekannten / nicht verwalteten Computer, Access Points oder andere Geräte im Netzwerk vorhanden

Patch Management

- ☐ Alle Server Patches werden zentral verwaltet und aktuell gehalten
- ☐ Alle Arbeitsplatz Patches werden zentral verwaltet und aktuell gehalten
- ☐ Alle anderen Betriebssysteme haben regelmäßige Patch-Wartung und sind aktuell
- ☐ Alle Applikationen und deren Patches werden gepflegt und aktuell gehalten
- ☐ Kontinuierliche Überwachung

Firewall

- ☐ Verwendung einer professionellen voll konfigurierten Firewall, keiner Endkunden Lösung
- ☐ Erweiterte Filterung, ‘intrusion detection’, ‘layer 7 traffic classification’
- ☐ Verwendung der neusten Version der Firewall-Software & kontinuierliche Updates
- ☐ Überwachen von Firewall Benachrichtigungen

Antivirus Software

- ☐ Verwendung einer professionellen Antiviren Software (AV), keiner Endkunden Lösung
- ☐ Auf allen Servern und Arbeitsplätzen läuft eine AV mit Echtzeit-Scanner
- ☐ Zentrale Verwaltung und Aktualisierung
- ☐ Richtlinien in AV, um die Ausführung von schädlichen ausführbaren Dateien zu blockieren, in Kombination mit Benachrichtigungen
- ☐ Überwachung von AV-Warnungen

Backups

- ☐ Aktives Backup Konzept
- ☐ Alle Maschinen, die über geschäftskritische Daten verfügen werden gesichert (idealerweise auf Medien auf die Windows keinen Zugriff hat)
- ☐ 3-2-1 Backup-Regel (3 Backups, auf 2 verschiedenen Medien gespeichert, 1 Offsite Sicherung)
- ☐ Image Sicherung von Servern werden mindestens monatlich durchgeführt
- ☐ Geschäftskritische Daten und Anwendungen werden täglich gesichert
- ☐ Einmal monatlich Restore Test durchführen
- ☐ Überwachen von Sicherungsfehlermeldungen
- ☐ Regelmäßige Aktualisierung der Backup Software

Filterung

- ☐ Aktiver Antispam/anti-phishing Filter
- ☐ Filtern von Dateianhängen in E-Mails (.exe, scr, .com, etc.)
- ☐ Aktiver DNS Filter
- ☐ Dateinamenerweiterungen in Windows anzeigen
- ☐ Aktivieren Sie keine Makros (für Microsoft Office-Dokumente)

Web Browser

- ☐ Deaktivieren Sie alle unnötigen Scripts / Plugins
- ☐ Browser und benötigte Plug-ins sind auf dem neusten Stand

Rechte

- ☐ Grundsatz der geringsten Privilegien / Rechte auf Systeme und Daten durchsetzen
- ☐ Software-Beschränkungsrichtlinien einführen um zu verhindern, dass Programme von gemeinsamen Ransomware-Standorten ausgeführt werden (Temp-Ordner usw.)

Erweiterte Vorbeugungsmaßnahmen

- ☐ Gruppenrichtlinien
- ☐ Periodischer Port / Schwachstellen Scan
- ☐ Überprüfen Sie das Netzwerk regelmäßig, um unnötige / anfällige Dienste zu deaktivieren

- Abgetrennte Netzwerkbereiche für Server, Backup, Daten & Arbeitsplätze (Stichwort Endpoint Protection)
- Deaktivieren Sie USB-Ports für Flash-Laufwerke usw.

Training

- Sicherheitstraining: Bieten Sie Beispiele an, was zu vermeiden ist (zB das Öffnen unbekannter Word / Excel Anlagen, etc)
- Simulierte Angriffe (Phishing etc.) mit Aktionsplan (zB: Trennen von Netzwerk / Wi-Fi)

NovaStor (www.novastor.de) ist der Hamburger Anbieter von Software für Datensicherung und -wiederherstellung. NovaStors Backup- und Restore-Software für kleine und mittelständische Unternehmen sichert einzelne Workstations und Server, aber auch kleine Windows-Netzwerke. Mit seinem gesamten Portfolio deckt NovaStor ein breites Anwendungsgebiet ab – vom mobilen Anwender über Fachabteilungen und mittelständische Unternehmen, bis zu internationalen Rechenzentren. Als deutscher Software-Hersteller steht NovaStor für höchste Qualität und Zuverlässigkeit. Die kostenoptimalen Lösungen von NovaStor sind hersteller- und hardwareneutral. Getreu seiner Philosophie „Backup wie für mich gemacht“ bietet NovaStor seinen Kunden die technisch und wirtschaftlich optimale Lösung zur Wiederherstellung ihrer Daten.

NovaStor ist inhabergeführt und mit rund 100 Mitarbeitern an drei Standorten in der Schweiz (Zug), Deutschland (Hamburg) und USA (Agoura Hills) sowie durch Partnerunternehmen in zahlreichen weiteren Ländern vertreten.