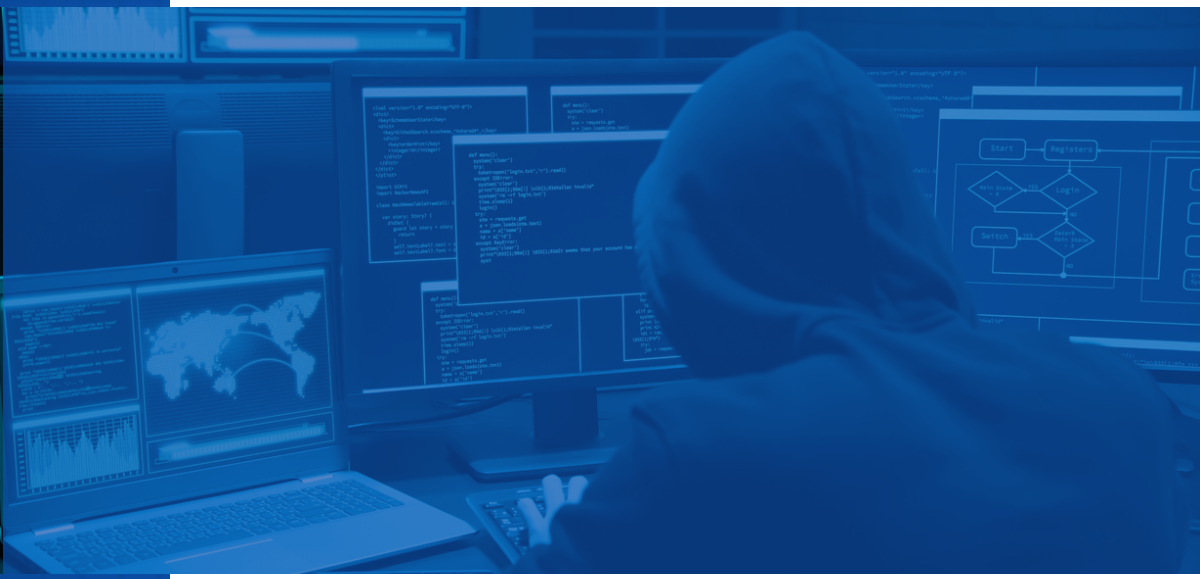
CHECKLISTE

NovaBACKUP



SO SCHÜTZEN SIE SICH VOR
RANSOMWARE

Ransomware-checkliste

Ransomware Vorbeugen

Ransomware stellt eine wachsende globale Bedrohung für Ihre Daten dar. Aber was ist Ransomware eigentlich? Ransomware ist eine bösartige Art von Malware, die Dateien auf Ihren Computern und Servern verschlüsselt und innerhalb von Minuten ein ganzes Netzwerk infizieren kann. Sobald Ihre Dateien verschlüsselt sind, fordern Cyberkriminelle ein Lösegeld in Form von Bitcoins, um Ihre Dateien wieder zu entschlüsseln. Im Jahr 2023 wurden beispielsweise mehr als 1 Milliarde US-Dollar an Cyberkriminelle gezahlt.

Ransomware wird nicht nachlassen und Sie sollten jetzt die notwendigen Schritte unternehmen, um sich zu schützen.

In dieser Checkliste finden Sie konkrete Beispiele für Maßnahmen, die Sie zur Minimierung des Risikos eines Ransomware-Angriffs ergreifen können und wie Sie im Falle eines Angriffs Ihre Systeme schnell und ohne Zahlung des Lösegelds wiederherstellen können.

Bestandsverwaltung

- [ ] Auflistung aller Software, die im gesamten Netzwerk eingesetzt wird.
- [ ] Betriebssysteme, die nicht mehr unterstützt werden (Windows 8, Server 2008, usw.), werden im Netzwerk nicht mehr ausgeführt.
- [ ] Die Nutzung von unseriöser Software ist unterbunden.
- [ ] 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 untergehen regelmäßiger Patch-Wartung und sind aktuell.
- [ ] Alle Applikationen und deren Patches werden gepflegt und aktuell gehalten.

Firewall

- [ ] Verwendung einer professionellen, voll konfigurierten Firewall.
- [ ] Erweiterte Filterung, z.B.: ‘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).
- [ ] Auf allen Servern und Arbeitsplätzen läuft eine AV mit Echtzeit-Scanner.
- [ ] Zentrale Verwaltung und Aktualisierung.
- [ ] Richtlinien in AV, die die Ausführung bösartiger Dateien blockieren, in Kombination mit Benachrichtigungsfunktionen.
- [ ] 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 mindestens täglich gesichert.
- [ ] Einmal im Monat wird ein Restoretest durchgeführt.
- [ ] Überwachen von Sicherungsfehlermeldungen.
- [ ] Regelmäßige Aktualisierung der Backup Software.

Filterung

- [ ] Aktiver Antispam/ Anti-Phishing Filter.
- [ ] Filtern von Dateianhängen in E-Mails (.exe, scr, .com, usw.).
- [ ] Aktiver DNS Filter.
- [ ] Dateinamenerweiterungen in Windows anzeigen.
- [ ] Aktivieren Sie keine Makros (für Microsoft Office-Dokumente).

Web Browser

- [ ] Deaktivieren Sie alle unnötigen Scripts/ Plug-ins.
- [ ] Browser und benötigte Plug-ins sind auf dem neusten Stand.

Rechte

- [ ] Prinzip der niedrigsten Rechte auf Datei- und Systemebene.
- [ ] Einführung von Software-Beschränkungsrichtlinien, 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 und deaktivieren Sie unnötige/ anfällige Dienste.

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

Training

- [ ] Sicherheitstraining: Informieren Sie über Themen, die Sie vermeiden sollten (z.B.: das Öffnen unbekannter Word/ Excel Anlagen, etc).
- [ ] Simulierte Angriffe (Phishing etc.) mit Aktionsplan (zB: Trennen von Netzwerk/ Wi-Fi).

ÜBER NOVABACKUP

Die NovaBACKUP Europe GmbH ist spezialisiert auf Backup und Disaster Recovery für Reseller und Managed Service Provider mit Fokus auf die Betreuung stark regulierter, professioneller Branchen. Mit über einer Million geschützten Maschinen und über zwanzig Jahren auf dem Markt, ist es das Ziel von NovaBACKUP, weltweit leistungsstarken, zuverlässigen und erschwinglichen Datenschutz zu bieten.

Weitere Informationen zu NovaBACKUP und unseren Produkten finden Sie unter https://www.novabackup.de

Sprechen Sie noch heute mit einem unserer Backup-Experten für eine kostenlose Beratung zu Ihrer Backup-Umgebung.

NovaBACKUP Europe GmbH
Marienstrasse 89, 30171 Hannover,
Deutschland

Tel.: +49 (40) 80811371
Email: kontakt@novabackup.de
www.novabackup.de