Checkliste
Ransomware - Notfall

Themen	erledigt	nicht zutreffend
Kernsysteme schützen		
Wenn möglich, Kernsysteme isolieren	☐	☐
Nutzerzugriff auf „geschäftskritische Systeme“ unterbinden/einschränken	☐	☐
Fileserver, Domain-Controller, Datenbanken schützen		
Schreibzugriff auf Dateien für alle Benutzer sperren (Skript nutzen, wenn verfügbar)	☐	☐
Benutzer mit den meisten geöffneten Dateien identifizieren	☐	☐
Fileserver in den Hibernations-Modus (Ruhemodus) versetzen, um den Arbeitsspeicher des Geräts zu erhalten	☐	☐
Notfallschritte am Gerät		
ACHTUNG: Auf KEINEN Fall am System mit Adminrechten anmelden, solange das Gerät noch im Netzwerk bzw. Internet ist	☐	☐
Trennen der Netzwerk- und sonstigen Kommunikationsverbindungen (LAN, Wi-Fi), im Zweifel über Deaktivieren des entsprechenden Ports am Netzwerk-Switch	☐	☐
Virtuelle Maschinen in den „Suspend-Modus“ versetzen (erhält Arbeitsspeicher)	☐	☐
Physikalisch Maschinen (PC) in den Standby-/Hibernations-Modus versetzen, um den Arbeitsspeicher des Geräts zu erhalten (Ruhezustand muss in Windows 10 erst aktiviert werden [Win10])	☐	☐
Lösegeldforderung und relevante Ereignisse mit einem Smartphone abfotografieren oder abfilmen. Dazu Gerät und Uhrzeit notieren, um das Bild im Nachgang korrekt zuordnen zu können	☐	☐
Notfallschritte im IT-Netzwerk		
Netzwerkverbindungen des Unternehmens nach außen trennen (Firewall, Internet)	☐	☐
Zwischen allen Netzwerksegmenten eine Src: ANY– Dest: ANY– Service: ANY– Action: Drop an die erste Stelle im Firewall-Regelset einfügen, damit Netzwerksegmente beim Wiederanlauf sukzessive „hochgefahren“ werden können	☐	☐
Netzwerkverbindungen zu Außenstellen kappen (MPLS, VPN, etc.); wenn Außenstellen bereits betroffen sind, sollten ggf. über die Firewalls per „Whitelisting“ nur dedizierte Notfall-Administrations-Verbindungen zugelassen werden, damit sich die Schadsoftware nicht unkontrollierbar in anderen Standorten verbreitet (Kontroll-Verlust)	☐	☐
Client-Remote-Zugänge abschalten	☐	☐
Interne Switches und Router abschalten, wenn keine Abschottung von Netzsegmenten möglich ist (z.B. Etagen-Switch, Router in das Fertigungsnetz)	☐	☐
Funknetze (Gäste, Mitarbeiter) abschalten, z.B. WLAN, 5G Campus Netz	☐	☐
IT-Endgeräte (Laptops, Server, PCs, Smart-TV, ClickShare, Beamer, Drucker, Massenspeicher) vom Netzwerk trennen	☐	☐

Checkliste
Ransomware - Notfall

Themen	erledigt	nicht zutreffend
Weitere Notfallschritte		
Alternative Kommunikationsinfrastruktur etablieren (z.B. Telefonkette), denn Angreifer könnten ggf. E-Mails mitlesen	☐	☐
Krisenstab etablieren, mit Mitgliedern aus IT, Kommunikation, Legal und Datenschutz	☐	☐
Keine E-Mails oder Dateien öffnen/weiterleiten, auch nicht über die Cloud, es könnten Geräte außerhalb des Netzwerkes (z.B. Privat-PC, Kunden, Lieferanten) infiziert werden	☐	☐
Mobile Dienstgeräte weder in privaten noch in geschäftlichen Netzen anmelden	☐	☐
Externe IT-Servicepartner umgehend informieren, z.B. Cloudanbieter	☐	☐
Keine eigenmächtigen ‚Reparaturversuche' ohne Nachfrage beim Spezialisten für die betroffenen Systeme.	☐	☐
Betroffene Systeme neu installieren oder auf einem Zustand vor der Infektion wiederherstellen, und unverzüglich absichern.	☐	☐
Saubere „Admin-Benutzer" anlegen und alle anderen (Admin-)Benutzer sperren	☐	☐
Anhalten von „Rotations-Prozessen" (Backup-Rotation, Log-Rotation, Snapshot-Rotation), damit keine weiteren Daten verloren gehen und sichern von System-Logs (Proxy, Firewall, Antivirus, Active-Directory, VPN, betroffene Systeme)	☐	☐
Nutzen von auf Grund des Vorfalls nicht arbeitsfähigen Mitarbeitern für andere Aufgaben (z.B. Koordination, Botengänge, Aushängen von Warnschildern)	☐	☐
Hinweise zur forensischen Untersuchung		
Damit die Möglichkeit einer forensischen Untersuchung bestehen bleibt, gibt es bestimmte Verhaltensregeln:	☐	☐
Auf KEINEN Fall Stromversorgung der IT-Systeme kappen	☐	☐
KEINE Dateien/Systeme löschen, selbst wenn sie von Malware infiziert sein könnten	☐	☐
Ein forensisches Backup (bitweise 1:1 Kopie) inklusive Speicherabbild für Strafverfolgung erstellen (lassen)	☐	☐
Grundsätzlich keine Software installieren. Wenn jedoch notwendig, die Quelle der Software und den Zeitpunkt der Installation dokumentieren	☐	☐
Protokoll über jeden Schritt erstellen, für jedes einzelne System vom Zeitpunkt der Identifizierung der Kompromittierung bis zum Abschluss der Arbeiten	☐	☐
Relevante Logdateien (Antivirus, Citrix, Login, Firewall, Webtraffic etc.) sicherstellen und vor Manipulation schützen	☐	☐
Spezialisten für forensische Untersuchungen hinzuziehen	☐	☐
Ist eine Cyberversicherung vorhanden, die Schadenhotline der Versicherung zwecks Unterstützung durch spezialisierte IT-Forensiker kontaktieren	☐	☐