Competence Center Industrial Security

VDMA Notfallhilfe
Ransomware

Inhalt

Vorwort

Steffen Zimmermann

Die Vorfälle mit Ransomware im Maschinen- und Anlagenbau haben in 2019 stark zugenommen. Es reicht nicht aus, sich dabei nur auf die Abwehr von Cyber-Angriffen zu fokussieren. Jedes Unternehmen muss davon ausgehen, dass früher oder später ein Angriff erfolgreich sein kann. Was nun zählt ist die schnelle Wiederherstellung eines sicheren Arbeitsmodus. Besonders kleine und mittelständische Unternehmen sind bedroht, fehlen doch hier oft die notwendigen Notfallvorsorgekonzepte und Krisenpläne, um bei Ransomware-Angriffen sofort zu wissen, welche Schritte zu tun sind.

Mit diesem Papier hat der VDMA Arbeitskreis „Informationssicherheit“ Antworten auf die grundlegenden Fragen nach einer Ransomware-Infektion zusammengeführt. Ergänzend dazu bietet das Papier eine Übersicht von Maßnahmen, Kontaktdaten und frei zugänglichen Informationen Dritter. Beachten Sie bitte auch die an diesem Papier beteiligten Mitgliedsunternehmen.

Steffen Zimmermann
VDMA Competence Center Industrial Security
Leiter des VDMA Arbeitskreises Informationssicherheit

1 Ziel/Scope

Dieses Dokument bietet betroffenen Unternehmen Hilfe bei einer Infektion mit Ransomware. Es gibt dafür Antworten auf die folgenden Fragen:

1. Woran erkenne ich einen Angriff?
2. Wann rufe ich einen Ransomware-Notfall aus?
3. Wie gehe ich im Ransomware-Notfall vor?
4. Was sollte ich vermeiden?
5. Wen kann ich im Notfall um Unterstützung bitten?
6. Welche Maßnahmen kann ich vornehmen, damit es nicht (nochmal) passiert?

Dieses Dokument betrachtet mögliche Abwehrmaßnahmen auf Basis einer „Ransomware Kill Chain“ im Maschinen- und Anlagenbau und stellt diese als Übersicht in einer Excel-Liste zur Verfügung.

Dieses Dokument richtet sich in erster Linie an IT-Leiter und IT-Sicherheitsbeauftragte mittelständischer Unternehmen, welche nicht über angemessene interne Ressourcen zu Ransomware verfügen.

Dieses Dokument formuliert keine verpflichtenden Vorgaben oder Anforderungen an den Schutz vor Ransomware, gibt jedoch Empfehlungen auf Basis von anerkannten Dokumenten unabhängiger Dritter.

Jeder Fall ist einzigartig, daher müssen alle Maßnahmen und Empfehlungen unter Berücksichtigung der individuellen Situation bewertet werden.

2 Definition eines Notfalls

Das BSI formuliert die Definition eines (allgemeinen) Notfalls wie folgt:

Ein Notfall ist ein Schadenereignis, bei dem Prozesse oder Ressourcen einer Institution nicht wie vorgesehen funktionieren. Die Verfügbarkeit der entsprechenden Prozesse oder Ressourcen kann innerhalb einer geforderten Zeit nicht wiederhergestellt werden. Der Geschäftsbetrieb ist stark beeinträchtigt. Eventuell vorhandene SLAs (Service Level Agreements) können nicht eingehalten werden. Es entstehen hohe bis sehr hohe Schäden, die sich signifikant und in nicht akzeptablem Rahmen auf das Gesamtjahresergebnis eines Unternehmens oder die Aufgabenerfüllung einer Behörde auswirken. Notfälle können nicht mehr im allgemeinen Tagesgeschäft abgewickelt werden, sondern erfordern eine gesonderte Notfallbewältigungsorganisation. [BSI 100-4]

Notfälle können auch durch Störungen hervorgerufen werden, welche nur mit außergewöhnlich hohem Aufwand zu beheben sind bzw. die einen unerwarteten oder nicht absehbaren Einfluss auf kritische Geschäftsprozesse, Kunden oder andere Bereiche haben, die von wesentlicher Bedeutung für das Unternehmen sind, z. B. der Verlust personenbezogener Daten nach der DSGVO, und so zu einem hohen Schaden für das Unternehmen führen.

Bei Überschreitung definierter Schwellenwerte ist ein Notfall auszurufen. Diese Schwellenwerte sollten Unternehmen nicht erst im akuten Fall bestimmen, sondern bereits im Vorfeld festlegen.

3 Ransomware Kill Chain

Auch wenn die eigenen IT-Systeme unsicher erscheinen, passieren Angriffe nicht „spontan". Jeder Angreifer muss sich für einen erfolgreichen Angriff gut vorbereiten. Eine plastische Illustration des „Angriffsplans" stellt die von Lockheed Martin entwickelte „Cyber Kill Chain" dar. Diese besteht auf aufeinander aufbauenden Stufen und beschreibt den immer tiefer ins Unternehmen führenden Weg des Angreifers. Aus der „Cyber Kill Chain" hat der VDMA Arbeitskreis die „Ransomware Kill Chain" abgeleitet. [CyberKillChain]

Die mit der „Ransomware Kill Chain" verbundene Übersicht über den Infektionsweg, betroffene Systeme und Auswirkungen lässt erkennen, an welchen Stellen geeignete Maßnahmen den weiteren Weg des Angreifers verhindert hätten. Für den Angriffsvektor „E-Mail" hat der VDMA Arbeitskreis auf Basis der „Ransomware Kill Chain" praxisnahe Maßnahmen abgeleitet. Die Details können der Excel-Datei entnommen werden. [VDMA-Excel-Killchain]

Die Excel-Liste und dieses Dokument zeigen mögliche Antworten auf die Frage „Was nun?", die am Ende der Ransomware Kill Chain auf alle betroffenen Unternehmen wartet.

Neben dem Infektionsweg „E-Mail" sind weitere Wege der Infektion denkbar, z. B. USB-Sticks, Laptops von Servicetechnikern, Mobiltelefone, ungesicherte Remotezugänge, ungepatchte Webserver usw. Dementsprechend können sich die Gegenmaßnahmen bei anderen Infektionswegen von den Maßnahmen, die in der Excel-Liste aufgeführt sind, unterscheiden.

Fallbeispiel Ransomware via E-Mail

Dieses Ablaufdiagramm beschreibt den klassischen Infektionsweg einer Ransomware via E-Mail. Maßnahmen zur Abwehr sind in der Excel-Liste aufgeführt. Die Beachtung und Umsetzung der Maßnahmen zeigt, wie der weitere Weg der Infektion verhindert werden kann.

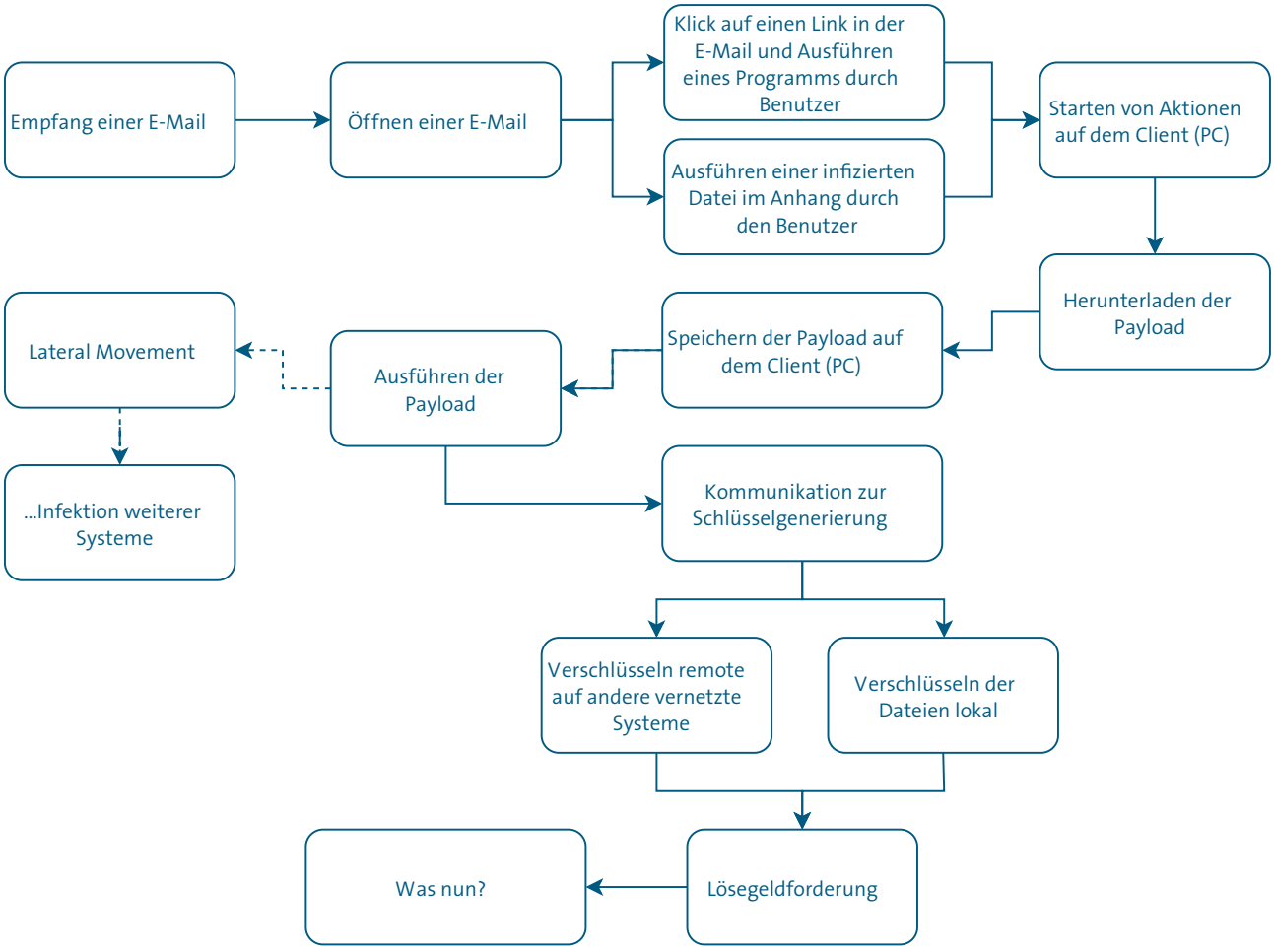

Abbildung 1: Ransomware Kill Chain

Quelle: VDMA

4 Woran erkenne ich einen Angriff?

Häufig erkennen nicht die Administratoren einen Angriff, sondern die Mitarbeiter. Nachfolgend beschrieben sind typische Indikatoren, die einen Ransomware-Vorfall als solchen erkennbar machen.

Indikatoren bei Mitarbeitern (Client-PC, Fileserver-Zugriff)

- Rechner wird langsam
- Entdeckung verschlüsselter bzw. nicht lesbarer Dateien
- Dateien lassen sich plötzlich nicht mehr öffnen
- unbekannte Dateien / Dateiendung
- Alarm des Virenscanners
- Neustart in den abgesicherten Modus
- Dateien mit Info/Anweisungen, dass ein Hack erfolgte (Lösegeldforderung)
- Lösegeld-Bildschirm-Meldung
- Lösegeld-Meldung bei Systemstart
- plötzliche Neustarts des Systems
- Anti-Virus-Software deaktiviert/ bringt Fehler und startet nicht
- Aufforderung zur Installation eines Programmes oder Eingabe des Administrator-Passworts
- Änderung des Desktophintergrunds
- E-Mails mit ungewöhnlichen oder unerwarteten Anhängen, Links, oder Aufforderungen, ungewohnte Dinge zu tun

Wir empfehlen grundsätzlich, dass Sie Ihre Mitarbeiter auf die Indikatoren „trainieren“. Zeigen Sie Ihnen, wie Ransomware- oder Phishing-Mails aussehen [Phishing]. Steigern Sie die Achtsamkeit. Bei verdächtigen Aktivitäten sollte umgehend der Systemadministrator (IT-Abteilung) bzw. der IT Helpdesk/Support angerufen werden. Die Nummer sollte allen Kolleginnen und Kollegen bekannt sein (und „offline“ verfügbar sein, da bei einem Ransomware-Angriff häufig kein Zugriff auf das Online-Adressbuch besteht). Rechnen Sie damit, dass im Notfall auch Ihre Telefonanlage betroffen sein kann.

Indikatoren für automatisierte Skripte (Administratoren)

- Typische verschlüsselte Dateien
- Typische Dateiendungen
- ausgehender Command&Control-Traffic auf der Firewall, IPS oder Websecurity-Gateway
- Blockierte Mails am Gateway (eventuell wurden einige zugestellt)
- Firewall deaktiviert/geändert
- Volumenschattenkopien sind alle gelöscht (viel weniger als üblich)
- Interne Hosts kommunizieren mit externen Hosts über ungewöhnliche Ports
- Kommunikation und/oder Alarme zu ungewöhnlichen (Geschäfts-)-Zeiten
- Verdächtige (interne) Netzwerk-Scans
- Häufung identischer verdächtiger Ereignisse
- Dubiose Log-in-Versuche eines Nutzers in das Firmennetzwerk (Login-Versuche von unterschiedlichen Orten innerhalb eines kurzen Zeitfensters)
- übermäßige Berechtigungsausweitung administrativer Konten und Änderung von Gruppenrichtlinien
- unbefugte Softwareinstallationen
- Identifikation und automatisches Löschen von Malware an mehreren Stellen gleichzeitig (dieser Vorgang wiederholt sich unendlich)
- ungewöhnlicher Verkehr von Servern in das Internet (Domaincontroller http, https o.ä.)
- Zugriffe auf ungenutzte Shares/Dateien („Canary Files“)
- Verschwinden, Fehlschlagen oder Unvollständigkeit von Backups

Die vollständige Liste der Indikatoren ist im Detail der Excel-Liste „Indikatoren“ zu entnehmen. [VDMA-Excel-Indikatoren]

Wichtig: Indikatoren können auf einen möglichen Angriff oder auf eine Infektion hinweisen. Auf diesen Angriff muss dann ggf. schnell reagiert werden. Diese „Incident Response“ kann jedoch Tagesgeschäft sein und ist nicht gleichzusetzen mit einem als Notfall deklarierten Ereignis.

5 Wann rufe ich einen Ransomware-Notfall aus?

Wie bei einem Verkehrsunfall gilt auch nach einem Cyber-Angriff: Ruhe bewahren und überlegt, aber zügig handeln! Hektischer Aktionismus kann im Zweifelsfall Ihren Schaden eher vergrößern, anstatt ihn in den Griff zu bekommen. Nicht jede, auch nennenswerte, Störung muss wie ein Notfall behandelt werden.

Feststellung eines Ransomware-Notfalls

Bei der Einschätzung, ob im konkreten Fall tatsächlich ein Notfall vorliegt, helfen folgende Fragen. Haben Sie alle Fragen mit „ja“ beantwortet, handelt es sich definitiv um einen Ransomware-Notfall.

Sind mehrere Systeme betroffen, so sollte zunächst davon ausgegangen werden, dass ein Großteil des Netzwerkbereiches betroffen ist. In flachen Netzstrukturen ohne Schutzzonen muss davon ausgegangen werden, dass das gesamte Netzwerk betroffen ist. Bei aktuellen Geschwindigkeiten verbreitet sich eine Schadsoftware oft in wenigen Minuten. Eine Verschlüsselung ist mit SSDs, Gigabit und leistungsfähigen Systemen auch oft in 1-2 Stunden abgeschlossen. Daher sollte schnell reagiert werden.

Faktor Schaden (Auswirkungen und Ausbreitung)

• Ist eine unkontrollierte Ausbreitung der Infektion (Verschlüsselung) im gesamten Netzwerk zu erwarten?	
• Sind kritische IT-Systeme oder Informationen nicht mehr verfügbar oder akut bedroht?	
• Sind kritische Geschäftsprozesse gestört oder akut bedroht?	

Faktor Zeit (Seit wann / wie lange noch?)

• Sind die Schritte und Zeitdauer zur Behebung des Vorfalls unklar?	
• Ist damit zu rechnen, dass die Dauer bis zur Wiederherstellung der Prozesse oder Systeme inakzeptabel ist?	
• Hat der Vorfall über die eigenen Prozesse, Dienste und Systeme hinaus signifikante Auswirkungen, z. B. in der Lieferkette des Kunden?	

Folgende weiterführende Fragen helfen bei der Konkretisierung eines Ransomware-Notfalls:

- Sind die Angreifer noch bei der Erkundung und Eroberung des Netzwerks?
- Werden Dateien noch verschlüsselt?
- Wurde bereits (alles) verschlüsselt?
- Sind privilegierte Konten betroffen?
- Kann die Störung eingegrenzt werden?
- Können die Aktivitäten lückenlos nachvollzogen werden?
- Sind andere Standorte betroffen?
- Ist bekannt, welche Maßnahmen zur Störungsbehebung zu ergreifen sind?
- Sind Backups der betroffenen Systeme verfügbar?
- Sind Ausweichszenarien denkbar (Mobilkommunikation statt Festnetz, Papier statt PDF, etc.)?
- Sind wesentliche Bereiche der Produktion ausgefallen?
- Ist die Qualität der Produkte betroffen?
- Ist die Lieferfähigkeit zu Kunden betroffen?
- Sind die Kommunikationswege kompromittiert?
- Sind weitere unkritische Funktionsbereiche betroffen (Kantine, Parkplätze)?
- Hat die Störung für Dritte erkennbare (Image-schädigende) Außenwirkungen, z. B. Ausfall des Webshops, keine telefonische Erreichbarkeit?
- Sind mit der Störung Meldepflichten (Behörden, Geschäftspartner u. a.) verbunden?

Hinweis zu Datenschutz (DSGVO): Eine Verletzung der Vertraulichkeit personenbezogener Daten beeinträchtigt nicht zwangsläufig interne Prozesse, kann aber erhebliche rechtliche Auswirkungen haben – zusätzlich zu möglichen Imageschäden. Der Verlust personenbezogener Daten muss zudem binnen 72 Stunden durch eine Meldung an die Aufsichtsbehörde angezeigt werden.

Auch der Verlust allgemeiner, aber sensibler, Unternehmensinformationen kann zu einem Notfall führen, beispielsweise, wenn diese Daten einem Konkurrenten zugespielt werden.

6 Wie gehe ich im Ransomware-Notfall vor?

Zuallererst ist **Ruhe zu bewahren.**

Besteht die Gefahr, dass infolge eines Angriffs, eines Bedienungsfehlers oder einer Manipulation die Funktionsfähigkeit des IT-Systems Schaden nimmt, ist der Entdecker aufgefordert, eigenständig Notfallmaßnahmen durchzuführen. Bei allen anderen Ereignissen erfolgt eine Meldung an den IT-Verantwortlichen bzw. IT-Support. Alle Aktivitäten sollten mit Zeitstempel, Verantwortlichem und Ablauf protokolliert werden. Eine vorbereitete Ransomware-Notfall-Checkliste kann diese Dokumentation erleichtern. Technische Ressourcen, wie z. B. Dateizugriffsüberwachung, AppLocker oder CryptoBlocker, sind in den VDMA Excel-Dateien gelistet.

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 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 Firewallregelset 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. Etagenswitche, 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

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
- Eigene Niederlassungen und IT-Personal an anderen Standorten informieren
- 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

Zur Erhaltung der Möglichkeit einer forensischen Untersuchung sind folgende Verhaltensregeln zu beachten:

- 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, Quelle der Software und 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

Etablierung eines Teams zur Ransomware-Notfallbewältigung

Notfallstab
Zur Notfallbewältigung sollte nach Entscheidung der Geschäftsführung einen Notfallstab gebildet werden. Der Notfallstab hat den Auftrag, die schnellstmögliche Wiederaufnahme des Geschäftsbetriebs zu gewährleisten und mögliche Folgeschäden auf ein Minimum zu begrenzen.

Mitglieder des Notfallstabs:
- Mitglied der Geschäftsführung und Stellvertreter
- Notfallbeauftragter nebst Stellvertreter
- Leiter IT bzw. IT-Sicherheit und Stellvertreter
- Bereichsleiter der betroffenen Organisationseinheiten
- Verantwortlicher für interne/ externe Kommunikation
- Ansprechpartner der für einen Notfall vorgesehenen externen Dienstleister

Lagezentrum
Die Mitglieder des Notfallstabs werden umgehend informiert und treffen sich an einem vom Notfallbeauftragten festgelegten Ort, dem Lagezentrum. Ausstattung, mögliche Zutrittsbeschränkungen sowie weitere Sicherheitsanforderungen des Lagezentrums sind dem BSI-Standard 100-4 Kapitel 7.1.3 zu entnehmen [BSI 100-4].

Kommunikation
Ein Notfall kann schnell von der Öffentlichkeit oder Kunden oder Wettbewerbern wahrgenommen und bewertet werden. Kommunikation ist daher einer der zentralen Erfolgsfaktoren der Notfallbewältigung. Sie umfasst die Kommunikation mit verschiedenen Interessengruppen während und nach einem Notfall mit dem Ziel, weiteren Schaden zu verhindern, zu informieren und Vertrauens- und Imageverluste zu vermeiden.

Folgende Vorgaben sind von allen Mitarbeitern zu berücksichtigen:

- Stellungnahme zu Medien und externen Personen ausschließlich durch den Kommunikationsverantwortlichen
- Mutmaßungen und Spekulationen sind zu vermeiden
- alle Anfragen zu Auskünften sind an das Lagezentrum weiterzuleiten

Deeskalation
- Nur der Notfallstab ist ermächtigt, den Notbetrieb zurückzunehmen
- Der Notfallstab informiert alle betroffenen Organisationseinheiten über die geplante Rückführung in den Normalbetrieb
- Ggf. erteilte Sonderbefugnisse werden wieder entzogen
- Die Leiter der Organisationseinheiten leiten in regelmäßigen Abständen eine Statusmeldung über den Fortschritt der Rückführung in den Normalbetrieb an den Notfallstab weiter
- Nach vollständiger und erfolgreicher Rückführung in den Normalbetrieb löst sich der Notfallstab auf

7 Was sollte ich vermeiden?

Typische Fehler im Umgang mit Ransomware sind:

Hektik und Aktionismus
Schnell sind Beweise zerstört, die Tätersuche dadurch erschwert. Sind Systeme vom Netzwerk abgekoppelt, stellen sie grundsätzlich keine Gefahr für andere Systeme mehr dar. Systeme in Quarantäne dürfen nicht wieder an das Netzwerk angeschlossen werden. Bei virtuellen Systemen lässt sich leicht der Zustand mit Snapshots (inkl. Arbeitsspeicher) sichern.

Holen Sie sich kompetente Unterstützung, bevor Sie ohne Erfahrung und aus Angst überreagieren. Nutzen Sie die Expertise von Außenstehenden nur, wenn Sie auf deren Verschwiegenheit vertrauen können.

Verharmlosung des Angriffs
Stellen Sie sicher, dass alle Mitarbeiter und Verantwortlichen, inkl. Geschäftsführung, über den Ernst der Lage informiert sind. Heimlichkeiten sorgen nur für größeren Schaden.

Annahmen statt Fakten
Entscheidungen aller Beteiligten sollten auf Fakten basieren. Systeme sind sauber? Es ist kein Innentäter, sondern ein Cyberangriff? Beweisen sie es! Nutzen Sie die Zeit, um Fakten zu sammeln.

Nicht abgestimmte Maßnahmen, Einzelaktionen
Stimmen Sie sich im Team mit den Systemverantwortlichen ab, fangen Sie nicht ohne Plan an. Sonst passiert es, dass sie ohne Not wieder von vorne anfangen müssen. Im Rahmen eines Sicherheitsvorfalles arbeiten verschiedene Interessen gegeneinander, zum Beispiel:

- Forensische Sicherung von Spuren
- Wiederherstellung von “funktionsfähigen” Daten und Systemen, kann aber Spuren vernichten
- Außenkommunikation
- Vertrauliches Vorgehen, um Ermittlungen nicht zu gefährden

Eine kontinuierliche Abstimmung der verschiedenen Tätigkeiten ist erforderlich.

Information außerhalb der definierten Eskalationswege
Gegenüber Kunden, Mitarbeitern und ggf. Presse darf es nur einen Kontakt geben, der „abgestimmte“ Informationen teilt. Darüber hinaus müssen die Kommunikationswege eingehalten werden, damit für Entscheidungen notwendiges Wissen rechtzeitig den Weg in das Lagezentrum findet. Zu viele Informationen können Ermittlungen stören oder weitere Angriffe herausfordern.

Lösegeld zahlen
Die Zahlen zeigen, dass je nach Statistik bis zu 70 % der Betroffenen zahlen. Sie sollten eine Zahlung um jeden Preis vermeiden. Dadurch erwecken Sie den Eindruck eines leichten Opfers, wodurch die Gefahr für Folgeangriffe massiv ansteigt. Zudem finanzieren Sie damit Folgeangriffe auf andere Opfer.

An infizierten oder unsicheren Systemen mit weitreichenden Berechtigungen anmelden (z. B. Domain Admin, lokaler Admin mit einheitlichem Kennwort oder root)
Bei vielen VDMA-Mitgliedern hat die Anmeldung des Admins erst zur Totalinfektion der gesamten Infrastruktur geführt. Bei infizierten Systemen muss davon ausgegangen werden, dass durch Keylogger, Rootkits oder per Token-Stealing die Zugangsdaten sofort für einen weiteren Verbreitungsweg und den Befall des Active Directories missbraucht werden.

Ungeprüfte Geräte ans Netzwerk anschließen
Starten Sie mit einem sicheren Kernnetz, in das nur verifiziert saubere Systeme aufgenommen werden. Sukzessive erweitern Sie das Netz. Vertrauen Sie dabei keinem Gerät, egal ob Laptop, Smartphone, Server oder Drucker. Nutzen Sie standardmäßig eine „Client-Firewall", um eingehende Verbindungen auf „Need to Access" beschränken.

Eilig heruntergeladene „Rettungstools" verwenden (Sekundärinfektion)
Nutzen Sie Tools nur dann, wenn Sie von vertrauenswürden Rechnern heruntergeladen wurden und von vertrauenswürdigen Partnern stammen, z. B. von Ihrem Antivirus-Hersteller oder von Microsoft. Sonst fangen Sie sich womöglich auf Ihren letzten sauberen Geräten eine neue Infektion ein.

Verschlüsselte Dateien voreilig löschen
Die Webseiten https://www.nomoreransom.org und https://id-ransomware.malwarehunterteam.com ermöglicht den Zugriff auf Entschlüsselungstools älterer Ransomware. Möglicherweise ist bereits eine Möglichkeit der Wiederherstellung vorhanden oder in einem vertretbaren Zeitraum verfügbar, ohne Lösegeld zu zahlen.

Infizierte Rechner ausschalten (aber unbedingt vom Netzwerk trennen – inkl. WiFi!)
Eventuell können technische Experten im Hauptspeicher noch den Verschlüsselungsmechanismus oder Verbreitungsweg identifizieren.

Voreiliger Upload von Dateien bei Cloud-Diensten (z. B. Virus Total, Hybrid-Analysis)
Der Upload von Dateien kann ein Informationsleak darstellen, da auf diese Dateien Partner der Dienstleister zugreifen können. Laden Sie nur Dateien hoch, die weder Betriebs- und Geschäftsgeheimnisse noch personenbezogene Daten enthalten. Ermitteln Sie ggf. den Hash-Wert der Dateien und fragen diesen bei den Dienstleistern ab.

Vorschnelles Wiederanfahren der Infrastruktur
Fahren sie die Systeme nicht voreilig wieder hoch. Es besteht ein berechtigter Wunsch der Geschäftsleitung, schnell wieder online zu gehen. Die Gefahr einer erneuten Infektion ist jedoch sehr hoch, solange nicht alle Systeme geprüft wurden. Die Erfahrung aus Infektionen im Maschinen- und Anlagenbau ist, dass bei einer umfassenden Ransomware-Infektion 4-6 Wochen bis zum Start der Produktivsysteme vergeht. Die Bearbeitung des gesamten Vorfalles beträgt aus IT-Sicht zwischen 6-9 Monate. Aus betriebswirtschaftlicher Sicht sind starke finanzielle Belastungen über mehrere Jahre einzuplanen.

8 Wen kann ich im Notfall um Unterstützung bitten?

Erste Hilfe zu Ransomware können Sie seitens Behörden, Interessensgemeinschaften oder Beratungsunternehmen erhalten. Die aktuellen Kontaktadressen finden Sie komprimiert im Anhang.

Behörden
Deutschsprachige Behörden können aktuell nur eingeschränkt Notfallhilfe zu Ransomware bieten. Insbesondere richtet sich das behördliche Notfall-Angebot vornehmlich an Infrastrukturbetreiber, deren Dienstleistungen für die Bevölkerung als kritisch angesehen werden (Sog. KRITIS). Folgende Behörden kommen für eine Unterstützung in Frage:

- Bundesamt für Sicherheit in der IT (BSI)
- Zentrale Ansprechstellen Cybercrime (ZAC) in den Landeskriminalämtern
- Lokale Schwerpunkt-Cybercrime-Dezernate (Kripo), sofern vorhanden
- Meldestelle MELANI (Schweiz)
- Meldestelle against Cybercrime (Österreich)

Zu Ransomware kann das ZAC im LKA Baden-Württemberg die landeseigene „Task Force Digitale Spuren“ einbringen. Nicht alle ZAC sind entsprechend auf Ransomware-Notfälle vorbereitet. Die Kontaktdaten zu den Behörden sind der Übersicht halber im Anhang zu finden.

Bestimmte Informationen können nur durch die Staatsanwaltschaft ermittelt werden. Daher ist eine zeitnahe Anzeige mit enger Abstimmung sinnvoll.

Interessensgemeinschaften / Cybersicherheits-Initiativen
Interessensgemeinschaften können einen Erstkontakt bieten und verweisen anschließend auf Partnerunternehmen der Privatwirtschaft.

- Allianz für Cyber-Sicherheit: Qualifizierte Dienstleister für APT-Response
- Cyberwehr BW: Notfallhilfe für Unternehmen in den Landkreisen Karlsruhe, Baden-Baden, Rastatt

Beratungsunternehmen
Dedizierte Spezialisten für IT-Security gibt es in vielen verschiedenen Beratungsunternehmen. Spezialisten für die schnelle Notfallhilfe bei Ransomware finden Sie im Anhang, darunter VDMA-Mitglieder und vom BSI zertifizierte APT-Dienstleister.

9 Welche Maßnahmen kann ich vornehmen, damit es nicht (nochmal) passiert?

Während eines Ransomware-Vorfalls sollten Sie nicht nur Notfall-Maßnahmen einleiten. Sie wollen schließlich keinesfalls dieselbe Informationstechnik wie vor dem Angriff. Es ist daher wichtig, dass Sie Ihre Infrastruktur mit höheren und den „richtigen“ Sicherheitsmaßnahmen aufbauen: Lessons learned. Selbstverständlich sind alle im folgenden genannten Maßnahmen auch als Präventiv-Maßnahmen bestens geeignet.

Generische Sofort-Maßnahmen

Der VDMA Arbeitskreis rät Ihnen, folgende Maßnahmen grundlegend und unabhängig des Angriffsvektors zu beachten und umzusetzen:

- Vermeidung/Abschaltung direkter Remote-Administration-Zugänge auf interne IT-Systeme, insbesondere RDP, Citrix, SSH
- Zwei-Faktor Authentisierung bei Systemen, die aus dem Internet erreichbar sind
- Deaktivierung von SMBv1 auf allen Systemen
- Patchmanagement von Betriebssystemen und Applikationen (z. B. PDF-Reader, Office, Bildbearbeitung, etc.)

Im Rahmen der Betrachtung des Angriffsvektors E-Mail (Ransomware Kill Chain) wurden Maßnahmen abgeleitet, die an spezifischen Punkten der Infektionskette den weiteren Weg verhindert hätten. Die vollständige Liste der Maßnahmen ist dem Excel-Dokument zu entnehmen [VDMA-Excel-Killchain].

Der VDMA Arbeitskreis hält die folgenden ausgewählten Maßnahmen für so wichtig, dass diese als verpflichtende Maßnahmen zur Umsetzung gefordert werden:

- Awareness-Training
- Kennzeichnung externer E-Mails
- Einschränkung von Nutzerrechten
- Konzept für Admin-Accounts (ggf. mit Microsoft LAPS)
- Blockierung potenziell gefährlicher Dateitypen
- Deaktivierung von unsignierten Office-Makros
- Netzwerksegmentierung
- Limitieren eingehender Verbindungen auf Clients
- Isolation von anfälligen Alt-Systemen (eigene Netzzone, dedizierte Admin-Gruppe)
- Internetzugang nur via Proxy-Server (mit Bedrohungsschutz)
- Limitierung von Remote-Zugängen, kein Direktzugriff via RDP, Citrix
- Blockierung des Netzwerkverkehrs in das / aus dem TOR-Netz (beide Richtungen)
- Regelmäßiges Backup & Offsite-Storage von Backupmedien
- Prüfung kritischer Systeme auf vollständige Wiederherstellbarkeit
- Entwicklung von „Kill-Switches“ für Kommunikationsverbindungen

Weiterführende Maßnahmen

Für eine nachhaltige Absicherung und Risikominimierung ist es notwendig, strukturiert die eigenen Gefährdungen zu ermitteln und auf Basis der Untersuchung aufeinander abgestimmte Maßnahmen zu etablieren. Dies umfasst Minimierung oder Vermeidung von Risiken, als auch deren Transfer (z. B. Versicherung) oder Akzeptanz.

Security-Checkliste abarbeiten
Basis-Checklisten helfen Ihnen, die richtigen Dinge anzupacken. Eine Vergleichbarkeit mit Unternehmen gleicher Größe oder Branche ist dabei wichtig. Wir empfehlen Ihnen hierfür den heise Security Consulter: https://www.heise-consulter.de/. Das Ergebnis ist ein für Sie passender Vergleich.

IT-Security Schutzkonzept nach BSI
Nachhaltiger als die Abarbeitung von Einzelmaßnahmen („Stopfen“ von Lücken) ist ein ganzheitliches IT-Sicherheitskonzept nach BSI Grundschutz, dass auch den Baustein zur Notfallvorsorge umfasst. Der BSI Grundschutz ist kostenfrei und bei mittelständischen Unternehmen im Maschinen- und Anlagenbau beliebt. Der Grundschutz umfasst zudem mit einem Baustein

für Industrielle Steuerungssysteme auch die Besonderheiten von Produktionsunternehmen. Einen gemeinsam mit VDMA-Mitgliedern erstellter digitaler Trainingskurs zur Umsetzung von Management-Maßnahmen bietet zudem die Online-Akademie University4Industry. [U4I]

Notfallplan erstellen (und verifizieren)
100 % Security gibt es nicht. Rechnen Sie damit, dass auch in Zukunft wieder ein Angriff erfolgreich sein könnte und Ihre ganze Infrastruktur in den Abgrund zieht. Bereiten Sie sich mit einem Notfallkonzept darauf vor. Die VSMA hat einen Muster-Notfallplan für Cyber-Angriffe auf Basis des BSI Bausteins Notfallmanagement (100-4) erstellt. Nutzen Sie dieses Muster, um Ihren individuellen Plan für den Notfall zu erarbeiten. [VSMA]

Die VSMA hat diese und weitere Hilfen von VDMA und VSMA auf der Webseite https://unternehmen-cybersicherheit.de zusammengeführt.

Zudem bietet die „IT-Notfallkarte“ des BSI eine gute Vorlage für den Aushang im Betrieb, um Mitarbeiter schnell über Meldewege und Grundmaßnahmen bei einem neuen „IT-Notfall“ zu informieren. [BSI-Notfall]

Cyberversicherung prüfen
Eine Versicherung wie die VDMA Cyber Police (VCP) kann grundsätzlich nur den entstandenen Schaden regulieren. Allerdings bieten alle Versicherungen die Möglichkeit, sich mit benannten Fachexperten zur Verbesserung der Cyberabwehr zusammen zu setzen. Auch Notfall-/Forensik-Dienstleister können vermittelt werden oder die Dienstleistung im Rahmen einer Cyberversicherung mit abgeschlossen werden. Die VDMA Cyber Police [VCP] bietet zudem einen auf die Eigenheiten von Produktionsunternehmen abgestimmten Versicherungsrahmen. Der Arbeitskreis Informationssicherheit hat gemeinsam mit der VSMA die Eignung der VCP in 16 typischen Szenarien geprüft. Die Szenarien und die Einschätzung der VSMA können vom VDMA oder der VSMA kostenfrei angefordert werden. [VCP-16]

Weiterführende Links zu Hilfen und Vorlagen finden Sie im nächsten Kapitel.

10 Weiterführende Informationen und Quellen

Nachfolgend finden Sie eine Übersicht von weiterführenden Informationen zu Ransomware und Incident Response.

Identifikation & Prävention

[VDMA-Excel-Killchain]	VDMA Ransomware Kill Chain – Infektion über E-Mail
[VDMA-Excel-Indikatoren]	VDMA Ransomware Indikatoren für eine mögliche Infektion
[VSMA]	Muster IT/Cyber-Notfallplan
[VCP]	VDMA CyberPolice (VCP)
[VCP-16]	16 Angriffs-Szenarien und Übernahme durch die VDMA CyberPolice (erhältlich via Biljana.Gabric@vdma.org)
[BSI]	Schutz vor Ransomware 2.0
[BSI 100-4]	BSI-Standard 100-4: Notfallmanagement
[IHK]	IHK-Leitfaden für IT-Notfälle (IHK NRW)
[NIST]	NIST Papier zu Security Incident Handling (en)
[GOVCERT]	GOVCERT Ransomware Countermeasures (en)
[CryptoBlocker]	CyptoBlocker für Ransomware-Dateitypen auf Windows Fileservern
[PowerShell]	PowerShell Security Best Practices
[AppLocker]	Windows AppLocker von Microsoft
[Phishing]	Informationen der Verbraucherzentrale zu Emotet
[U4I]	Online Trainingskurs für Management von Industrial Security
[CyberKillChain]	Lockheed Martin Cyber Kill Chain
[ProcessBouncer]	Proof of Concept für einen Process Bouncer von Holger Junker (BSI)

Simulation & Detektion

[KnowB4]	KnowB4 Software zur Simulation eines Ransomware-Angriffs
[EmoCheck]	Tool zum Aufspüren von Emotet-Infektionen

Reaktion & Wiederherstellung

[Win10]	Windows 10 Ruhezustand aktivieren
[BSI-Ersthilfe]	Erste Hilfe bei einem schweren IT-Sicherheitsvorfall
[BSI-Notfall]	IT-Notfallkarte
[aramido.de]	Ransomware Krisenplan
[NoMoreRansom]	No More Ransom – Entschlüsselungstools
[CyberWehr]	https://cyberwehr-bw.de/ für Unternehmen in Baden-Württemberg

11 Redaktionskreis

Aus der Praxis für die Praxis. Die Kollegen aus dem VDMA Arbeitskreis „Informationssicherheit“ arbeiten aktiv an produktiv verwendbaren Dokumenten. Zudem kümmert sich der Arbeitskreis um Einschätzungen zu aktuellen Sachverhalten, greift Zukunftsthemen auf und nutzt das Netzwerk der IT-Security-Verantwortlichen im VDMA zum informellen Erfahrungsaustausch.

Aktive Autoren

Andreas Behncke
Dürr IT Service GmbH

Dr. Ralf Behnke
Umicore AG & Co. KG

Florian Buschor
Syntegon Packaging Systems AG

Alexandra Dauscher
TROX GmbH

Dr. Thomas Demuth
Vaillant GmbH

Stefan Ditting
HIMA Paul Hildebrandt GmbH

Marco Jaßniger
Wilhelm Bahmüller Maschinenbau Präzisionswerkzeuge GmbH

Maximilian Korff
Siemens AG

Jochen Müller
Bizerba SE & Co. KG

Henrik Mündörfer
Dieffenbacher GmbH
Maschinen- und Anlagenbau

Olaf Nothdurft
KARL MAYER Holding GmbH & Co. KG

Dr. Thomas Nowey
Krones AG

Thorsten Sauer
viastore SYSTEMS GmbH

Jan Sahlke
Hauni Maschinenbau GmbH

Denis Schröder
Bühler Technologies GmbH

Markus Stäudinger
Maschinenfabrik Eirich GmbH & Co KG

Stefan Sommer
RENK AG

Kevin Wallis
TRUMPF Laser GmbH

Gunther Vaßen
ifm electronic GmbH

Uwe Zetzmann
Kaeser Kompressoren SE

Steffen Zimmermann
VDMA e. V.

VDMA AK „Informationssicherheit“

Sprecher: Rolf Strehle, Voith

VDMA e. V.
Abteilung Informatik
Lyoner Straße 18
60528 Frankfurt am Main

Stand: 28.01.2020

12 Anhang: Kontaktstelle, Excel-Listen

Behörden

Grundsätzlich dienen die Zentralen Ansprechstellen Cybercrime (ZAC) als erste Kontaktstelle. Sollte die ZAC in Ihrem Bundesland keine Hilfe sein, so können Sie alternativ das BKA oder das BSI CERT Bund um Hilfe bitten. Leider stellt die Meldestelle für Cybercrime in der Schweiz keine Telefonnummer für den Notfall bereit.

Land/Bund	Telefonnummer	E-Mail-Adresse
MELANI (Schweiz)	[keine]	https://www.melani.admin.ch/ (Formular)
BKA Meldestelle (Österreich)	01 24836-985025	against-cybercrime@bmi.gv.at
BSI CERT Bund	0228 99 9582 222	certbund@bsi.bund.de
Bundeskriminalamt	0611 55-15037	zac@cyber.bka.de
Baden-Württemberg	0711 5401-2444	cybercrime@polizei.bwl.de
Bayern	089 1212-3300	zac@polizei.bayern.de
Berlin	030 4664-924924	zac@polizei.berlin.de
Brandenburg	03334 388-8686	zac@polizei.brandenburg.de
Bremen	0421 362-19820	cybercrime@polizei.bremen.de
Hamburg	040 4286-75455	zac@polizei.hamburg.de
Hessen	0611 83-8377	zac.hlka@polizei.hessen.de
Mecklenburg-Vorpommern	03866 64-4545	cybercrime.lka@polmv.de
Niedersachsen	0511 26262-3804	zac@lka.polizei.niedersachsen.de
Nordrhein-Westfalen	0211 939-4040	cybercrime.lka@polizei.nrw.de
Rheinland-Pfalz	06131 65-2565	lka.cybercrime@polizei.rlp.de
Saarland	0681 962-2448	cybercrime@polizei.slpol.de
Sachsen	0351 855 – 3226	zac.lka@polizei.sachsen.de
Sachsen-Anhalt	0391 250-2244	zac.lka@polizei.sachsen-anhalt.de
Schleswig-Holstein	0431 160-4545	cybercrime@polizei.landsh.de
Thüringen	0361 341-4545	cybercrime.lka@polizei.thueringen.de

Die aktuelle Liste der Kontaktstellen in Deutschland finden Sie hier:
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Meldestelle/Polizeikontakt/ZACkontakt/zackontakt.html

Kontaktstellen von VDMA-Mitgliedern

Folgende Mitgliedsunternehmen des VDMA Fachverbands „Software und Digitalisierung“ haben bereits Erfahrungen im Umgang mit Ransomware-Notfällen im Maschinen- und Anlagenbau.

Firma	Ort	Kontakt	Notfall-Nummer*
@-yet GmbH	Leichlingen (NRW)	Wolfgang Straßer	+49 163 5 55 65 56
Konica Minolta Business Solution GmbH	Stuttgart	security-support@konicaminolta.de	+49 711 1385 399
Hi-Solutions	Berlin	Prof. Timo Kob	+49 172 3 90 75 09

*Kontaktzeiten sind, wenn nicht anders angegeben, jeweils 08:00 – 17:00 Uhr

BSI-zertifizierte Unternehmen für APT-Angriffe

Das BSI hat gemäß § 3 BSIG die Aufgabe, Betreiber Kritischer Infrastrukturen auf deren Ersuchen bei der Sicherung ihrer Informationstechnik zu beraten und zu unterstützen. Hierzu kann auch auf qualifizierte Sicherheitsdienstleister verwiesen werden. Die Qualifizierung zum sogenannten „APT-Response Dienstleister“ haben folgende Unternehmen durchlaufen:

Firma	Notfall-Kontakt	Name
BFK edv-consulting	+49 721 962011	cfischer@bfk.de
Corporate Trust	+49 89 599 88 75 80	info@corporate-trust.de
DCSO	+49 30 726219 0	incident@dcso.de
HiSolutions	+49 30 533289 0	info@hisolutions.com
QuoScient	+49 69 33 99 79 38	threatops@quoscient.io
SySS	+49 7071 407856 40	csirl@syss.de
T-Systems / Telekom Security	+49 89 545506105	alexander.schinner@t-systems.com
Warth & Klein Grant Thornton AG	+49 211 9524 8824	helmut.brechtken@wkgt.com

(Stand: Januar 2020)

Die „APT-Response Dienstleister“ wurden durch das BSI anhand transparenter Kriterien und Verfahren qualifiziert. Dies beinhaltet neben der Veröffentlichung von Kontaktdaten die Gegenüberstellung einzelner Leistungsmerkmale der Dienstleister. Das BSI-Dokument mit den Auswahlkriterien, den Leistungsmerkmalen und der Gegenüberstellung finden Sie hier:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister_APT-Response-Liste.pdf

Ransomware Indikatoren

Stand: 28.01.2020

		Auf welchem Gerät?			Erkennung	
Indikatoren	**auto-mati-sierbar?**	**Client**	**Fileserver (Explorer)**	**Server (OS)**	**User**	**Power User**
Rechner wird langsam		x		x	x	x
Entdeckte verschlüsselte Dateien	x	x	x	x	x	x
Dateien lassen sich plötzlich nicht mehr öffnen		x	x	x	x	x
Unbekannte Dateien	x	x	x	x	x	x
Dateien mit Info/Anweisungen, dass ein Hack erfolgte (Lösegeldforderung)		x	x	x	x	x
Unbekannte, neue Prozesse im Task-Manager		x		x		x
Unbekannte, neue Benutzer im Task-Manager		x		x		x
Autostart-Einträge	x	x		x		x
Registry-Run Einträge	x	x		x		x
Dienste		x		x		x
Alarm eines Virenscanners	x	x		x	x	x
Ausgehender C2-Traffic auf der Firewall	x	x		x		
Zugriff auf komische/unbekannte URLs	x	x		x		
Info vom Mitarbeiter, dass er geklickt hat		x			x	x
Blockierte Mails am Gateway (eventuell wurden einige zugestellt)	x			x		
Lösegeld-Bildschirm-Meldung		x		x	x	x
Lösegeld-Meldung bei Boot		x		x	x	x
Plötzliche Neustarts des Systems?		x		x	x	x
Anti-Virus-Software deaktiviert/ bringt Fehler und startet nicht	x	x		x	x	x
Aufforderung zur Installation eines Programmes oder Eingabe des Administrator-Passworts		x		x	x	x
Änderung des Desktophintergrunds		x		x	x	x
E-Mails mit ungewöhnlichen oder unerwarteten Anhängen, Links, oder Aufforderungen, ungewohnte Dinge zu tun	x	x			x	x
IDS-Events	x	x		x		
SIEM-Events	x	x		x		
Firewall deaktiviert/geändert	x	x		x	x	x
Anti-Virus-Software deaktiviert/bringt Fehler und startet nicht		x		x	x	x
Volumenschattenkopien sind alle gelöscht (viel weniger als üblich)	x			x		
Interne Hosts kommunizieren mit bösartigen oder unbekannten Zieladressen	x	x		x		
Interne Hosts kommunizieren mit externen Hosts über ungewöhnliche Ports	x	x		x		
Kommunikation und oder Alarme zu ungewöhnlichen (Geschäfts-)Zeiten	x			x		
Öffentlich zugängliche Hosts oder Hosts in entmilitarisierten Zonen (DMZ) kommunizieren mit internen Hosts	x			x		
Verdächtige (interne) Netzwerk-Scans	x	x		x		
Häufung identischer verdächtiger Ereignisse	x	x	x	x	x	x
Schnelle Re-Infektion mit Malware nach Beseitigung kann auf Rootkit bzw. unvollständige Bereinigung (z.B. Dropper wird nicht erkannt) hindeuten		x		x		
Dubiose Log-in-Versuche eines Nutzers in das Firmennetzwerk (Loginversuche von unterschiedlichen Orten innerhalb eines kurzen Zeitfensters)	x			x		
Übermäßige Berechtigungsausweitung administrativer Konten und Änderung von Gruppenrichtlinien	x	x		x		
Unbefugte Softwareinstallationen	x	x		x		
Zugriff auf Canary-Files/Shares	x	x	x	x		
Plötzlicher Anstieg von Aktivität auf NAS-Speichern durch mehrere Systeme	x			x		
Verschwinden, Fehlschlagen oder Unvollständigkeit von Backups	x		x	x		
Identifikation und automatisches Löschen von Malware an mehreren Stellen gleichzeitig (dieser Vorgang wiederholt sich unendlich)	x	x	x	x		
Ungewöhnlicher Verkehr von Servern in das Internet (Domaincontroller http, https o.ä.)	x			x		

Zeitfenster seit Erstinfektion		Eignung			
Manuell	**Automatisiert**	**Aware-ness**	**IoC Skript**	**Vermeid-bar?**	**Empfehlung**
Minuten*	-	x			
Minuten*	Sekunden	x	x	x	Client: Windows Ransomware-Schutz einschalten Fileserver: FSRM einschalten, Benutzer sperren [fsrm] [cryptoblocker]
Minuten*	-	x			
Minuten*	Sekunden	x	x	x	FSRM einschalten und konfigurieren [fsrm] [crpytoblocker]; File Extention Liste nutzen [fel]
Minuten*		x			
Forensik				x	Application Whitelisting mit AppLocker [applocker]
Forensik					
Forensik	Sekunden		x		
Forensik	Sekunden		x		
Forensik					
Stunden	Stunden	x	x		
Forensik	Sekunden		x	x	Nutzung von C2-Listen bekannter Server-Ips [C2-List] Surfen nur via Webproxy, direkte Internetverbindung vermeiden; Webzugriff von Servern nur stark eingeschränkt auf z.B. Windows Update
Forensik	Sekunden		x	x	Surfen nur via Webproxy, direkte Internetverbindung vermeiden; Webzugriff von Servern nur stark eingeschränkt auf z.B. Windows Update
Minuten*		x			
Forensik	Sekunden		x		
Minuten*		x			
Minuten*		x			
Minuten*		x			
Minuten*	Sekunden	x			
Minuten*		x			
Minuten*		x			Kann auch durch Energieeinspareinstellungen kommen (Fals Positive)
Minuten*		x	x	x	Mitigation durch Dateifilter, auch durch Microsoft Power Automate (Flow)
Forensik	Sekunden		x		
Forensik	Sekunden		x		
Forensik	Sekunden		x		
Minuten*		x	x		
Forensik	Sekunden		x	x	Deaktivierung von vssadmin.exe via AppLocker [vssadmin]
-	Minuten		x	x	Surfen nur via Webproxy, direkte Internetverbindung vermeiden; Webzugriff von Servern nur stark eingeschränkt auf z.B. Windows Update
-	Sekunden		x	x	Unterbinden in der Firewall, Automatisierter Lockdown
-	Minuten		x		Abhängig vom Geschäftsfeld des Unternehmens
-	Sekunden		x	x	Unterbinden in der Firewall
-	Sekunden		x	x	Unterbinden in der Firewall, Automatisierter Lockdown
Minuten*	Minuten	x	x		IT-Support sollte auf Beachtung von möglichen Korrelationen von Ereignissen vorbereitet werden
Stunden					
Forensik	Minuten		x	x	Automatisierter zeitabhängiger Lockdown eines Nutzerkontos
Forensik	Sekunden		x		
Forensik	Sekunden		x	x	Application Whitelisting mit AppLocker [applocker]
Forensik	Sekunden		x		
Forensik	Sekunden		x		
Tage	Sekunden		x	x	Backup- und Restore mit individuellen Konten und Berechtigungen versehen, FSRM nutzen um Löschen/Verändern von Backups festzustellen
Forensik	Sekunden		x		
Forensik	Minuten		x		Anomaly Detection

*zu Geschäftszeiten

Ransomware-Kill-Chain

Stand: 21.01.2020 • Use Case: Angriff via E-Mail • © VDMA e.V.

Hauptannahmen

Den nicht informierten User trifft keine Schuld/Das Netzwerk kann nicht abgeschaltet werden/E-Mails müssen empfangen werden/Ransomware-Angriffe funktionieren auf voll gepatchten Systemen/Ein Schutz kann nur durch gestaffelte Maßnahmen erreicht werden

Angriffsschritte	Risiken	Pflicht?	Maßnahmen
Empfang einer Email	R: Faken des Absenders		M: DNS & IP-Tools: Nutzung von SPF, DKIM, DMARC, E-Mail-Blacklists, Spamcop, etc.
			M: DNAE Domain Named Authenticated Entities
			M: Einschränken der „Spam-Authentizität“ (wie echt können gefälschte Emails aussehen)
		ja	M: Awarenesstraining: Nicht auf einfach fälschbaren „Display Namen“ verlassen
		ja	Markierung einer externen Mail als „Extern“
	R: E-Mail mit ausführbarer Datei im Anhang	ja	M: gefährliche Dateitypen blocken, mind. ausführbare Dateien
	R: E-Mail mit aktivem Inhalt im Anhang (Office z.B.)		M: Einschränkung der Empfangsrechte auf spezifische Gruppen
			M: Makros in Officedateien beim Empfang automatisiert entfernen
			M: BSI-Empfehlung zu Gruppenrichtlinien für Microsoft Office umsetzen
			M: Nur signierte Makros oder weniger in Office zulassen
Öffnen einer E-Mail	R: Öffnen einer privaten Mail über Webmailer		M: Sensibilisierung der User; organisatorische Richtlinie
	R: Der Anhang enthält eine ausführbare Datei		M: Empfang von ausführbaren Dateien einschränken
Ausführen einer geskripteten Datei durch den User	R: funktioniert auf voll gepatchten Systemen, da die User die Datei ausführen		M: Heuristik / „KI“ des Antivirus-Programms nutzen
			M: Verhaltensbasierte Analyse/Abwehr
			M: Sandboxing (Gateway)
		ja	M: Deaktivieren von Office Makros per Gruppenrichtlinie, Aktivierung nur für ausgewählte User
Starten von Aktionen auf dem Client	R: User hat umfassende Rechte	ja	M: Kein angemeldeter Benutzer hat Adminrechte
Herunterladen der Payload	R: Herunterladen im Hintergrund nicht sichtbar	ja	M: Internetzugang nur via Proxy oder NGFW mit Deep Packet Inspection
	R: Download von ausführbarer Datei		M: Ausführbare Dateien nur nach Bestätigung eines Dialogs herunterladbar
		ja	M: Ausführbare Dateien im Download blocken
	R: Download von spezifischen Payload-Seiten		M: Nicht benötigte IP-Adressbereiche blocken
			M: Nicht benötigte DNS-Bereiche blocken (?)
		ja	M: TOR-Netz blockieren
		ja	M: Blacklists für bekannte IOC einspielen (Bspw. Emotet) sofern System/Proxy vorhanden
	R: Herunterladen von spezifischer Malware	ja	M: Blockieren bekannter Dateitypen
			M: Überwachung von Netzwerkaktivitäten, z.B. durch SIEM
			M: Aktivieren von Sandbox-Verfahren im Webfilter
			M: Erkennung & Block durch Virenscanner mit Intrusion Prevention
Speichern der Payload auf dem Client	R: Speicherung unerkannter Malware		M: Application Directory Whitelisting (Schreibrechte deaktivieren)
Ausführen der Payload	R: Ausführen von Malware		M: Application Whitelisting
	R: Ausführung von Dateien in bestimmten Verzeichnissen		M: Temp-Verzeichnisse einschränken via AppLocker/ Software Restriction Policies
		ja	M: Geschützte Ansicht bei Office-Dokumenten Aktivieren in TEMP und Downloadverzeichnissen
	R: User hat Adminrechte		M: Adminrechte in dedizierten Account verschieben
		ja	M: tägliches Arbeiten nur ohne Adminrechte
	M: Kommunikationsbeziehungen in lokaler Firewall einschränken		M: SMB/SMTP/...-Kommunikation auf freigegebene Anwendungen einschränken

Maßnahmen unabhängig vom Angriffsvektor „E-Mail“
Vermeidung direkter Remote-Administration-Zugänge auf interne IT-Systeme (z.B. RDP, Citrix, SSH, etc.)/Zwei-Faktor Authentisierung bei Systemen, die aus dem Internet erreichbar sind/Deaktivierung von SMBv1 auf allen Systemen/Patchmanagement von Betriebssystemen und Applikationen (z.B. PDF-Reader, Office, etc.)

	Einschätzung VDMA					
	Einrich-tung	Pflege	Nutzen	Umsetz-bar?	Umge-setzt?	Verant-wortlich
Kommentare zu Maßnahmen	1=geringer Aufwand		5=hoch			
Blacklists müssen regelmäßig gepflegt werden, für Kunden sollten Ausnahmen definiert werden können	4	2	5			
Zertifikatsprüfung durch den Absender	4	2	3			
Mailserver so konfigurieren, dass SPAM für Nutzer einfach erkennbar wird	2	2	3			
Nachhaltig nur durch Wiederholung, auch für neue Mitarbeiter	5	3	4			
Ablehnende Haltung von Vertriebsmitarbeitern	1	1	3			
https://www.govcert.ch/downloads/blocked-filetypes.txt	1	1	3			
Gefahr des Dauerzustands für alle Mitarbeiter	3	2	2			
schwierig umzusetzen, fehlerhafte Dateien möglich	5	1	2			
sehr umfangreich	4	3	4			
Standardeinstellung in Office	1	1	3			
Evtl. auch automatisiert via Webfilter einschränken	2	2	2			
	1	1	3			
Statistik: 10% der User klicken auf eine Phishing-Mail	2	2	3			
Ist meist bei Next Generation AV integriert	2	2	3			
Angreifer können Sandboxing erkennen	3	3	3			
Ablehnende Haltung der Mitarbeiter da viel selbst gestricktes im Umlauf	1	3	3			
Ausbreitung auf Systeme mit Schreibrechten begrenzt	2	1	4			
Proxyserver kann gleichzeitig Dateiinhalt prüfen - https-Traffic aufbrechen	3	3	3			
Stärkt Awareness, Proxy bzw. Webfilter notwendig	3	3	2			
Ausnahmen beschäftigen die IT-Abteilung stark	2	4	3			
Sperre hilft auch bei anderen Angriffen, sollte ergänzend auch dynamisch erfolgen	2	2	3			
Alternative DNS-Server blockieren	2	1	2			
Könnte reguläre Kommunikation blocken	3	2	2			
	2	2	3			
Ausnahmen beschäftigen die IT-Abteilung	2	2	3			
Auswertung muss eingeplant werden	4	3	4			
Angreifer können Sandboxing erkennen	2	2	3			
Ist meist bei Next Generation AV integriert	2	2	3			
Zusätzliche Überwachung auf Verschlüsselung mit Windows Bordmitteln	3	3	4			
schwierig, da hoher Konfigurations- und Pflegeaufwand; empfohlen für Nicht-Patchfähige oder stabile Systeme	3	3	4			
schwierig, da hoher Konfigurations- und Pflegeaufwand; empfohlen für Nicht-Patchfähige oder stabile Systeme	3	3	3			
Verhindert nicht die automatische Ausführung	1	1	2			
Verhindert nicht die Ausführung des Schadcodes	3	3	3			
	3	3	3			
Verhindert das Ausbreiten, aber nicht die Erstinfektion	3	2	3			

Ransomware-Kill-Chain

Stand: 21.01.2020 • Use Case: Angriff via E-Mail • © VDMA e.V.

Angriffsschritte	Risiken	Pflicht?	Maßnahmen
Verbreitung / Lateral Movement	R: Ausnutzen (un)bekannter und ungepatchter Schwachstellen		M: Regelmäßige Installation von Sicherheitsupdates
			M: Basismaßnahmen zum Härten der Systeme umsetzen
			M: Microsoft Tier Model für die AD-Architektur umsetzen
	R: Angreifer erlangt Privilegien durch Admin-Anmeldung		M: Abschalten von WDigest Caching, Credential Caching, ..
			M: Einschränkung von vererbten/delegierten Berechtigungen
			M: Zugriffe „privilegierter Accounts“ gegen andere Sicherheitsbereiche (Clients,Server,Domäne) verbieten.
			M: M: Verwenden eines dedizierten Kontos für die lokale Verwaltung (z.B. LAPS) anstelle eines allgemeinen Kontos für alle Geräte
Kommunikation zur Schlüsselgenerierung	R: verschlüsselte Kommunikation mit C2-Server		M: Proxyanmeldung einschalten mit Zertifikatsprüfung
			M: Kommunikation mit bekannten C2-Servern unterbinden
Verschlüsseln der Dateien lokal	R: Alle Dateien lokal werden verschlüsselt		M: Clients vom Netz nehmen
			M: Virtuelle Maschinen pausieren oder „Snapshot mit Memory erstellen“
			M: Forensisches Backup des betroffenen Rechners
			M: Prüfung wichtiger Ordner auf verdächtige Aktivitäten
Verschlüsseln remote	R: Zugriff mit den Rechten des Users	ja	M: Schreibrechte einschränken
		ja	M: Netzwerk segmentieren, um Zugriff auf andere Systeme zu vermeiden
	R: wichtige Daten werden verschlüsselt	ja	M: regelmäßige Backups von Systemen
		ja	M: Offsite Storage von Backups; Lagerung an einem anderen Ort
			M: (regelmäßige) Tests der Backup
		ja	M: Prüfung kritischer Systeme auf vollständige Wiederherstellbarkeit
			M: Finden des Patient Zero
			M: Aufbewahren verschlüsselter Dateien
			M: Überwachung von Netzwerkaktivitäten durch SIEM
			M: Skripte für das Erkennen von Ransomware-Dateiendungen und Zugriff auf Canary-Files/-Shares installieren
			M: Skripte installieren, um gefährliche Clients bei Entdeckung auszusperren
	Sofortmaßnahmen definieren	ja	M: Deaktivieren von Verbindungen zu anderen Standorten vorbereiten
			M: Recht zur Abschaltung von Netzwerkkomponenten an lokale Verantwortliche delegieren
			M: Skript vorbereiten, um Schreibrechte auf Storagesystemen automatisiert zu deaktivieren
Lösegeldforderung			M: Bildschirm abfotografieren / Screenshot
			M: Anzeige erstatten
			M: LKA ZACs anfragen/informieren
			M: BSI Lagezentrum anrufen
Bezahlung			M: Da nicht sichergestellt werden kann, dass nach erfolgter Lösegeldzahlung die Daten auch tatsächlich freigegeben werden, raten wir grundsätzlich von einer Zahlung ab.

	Einschätzung VDMA					
Kommentare zu Maßnahmen	**Einrich-tung** 1=geringer Aufwand	**Pflege**	**Nutzen** 5=hoch	**Umsetz-bar?**	**Umge-setzt?**	**Verant-wortlich**
Verhindert das Ausbreiten, aber nicht die Erstinfektion	4	2	4			
Win10: nach BSI-Projekt „SiSyPHuS Win10“	4	3	4			
Mindestens für Tier 0	4	2	3			
Anzahl der Cached Credentials auf „1“ bei Laptops	2	1	2			
schwierig, da hoher Konfigurations- und Pflegeaufwand	4	4	2			
am besten individuelle Zugriffe freischalten	4	3	3			
Microsoft LAPS ist für AD-verwaltete Geräte	3	2	2			
Verbindung zu unbekannten self-signed Zertifikaten unterbinden, lange Liste von Ausnahmen notwendig	3	3	2			
Nutzung von Online-Listen bekannter Server	3	2	2			
Zeit ist Geld. Gerät grundsätzlich eingeschaltet lassen, um forensische Untersuchung zu ermöglichen	2	2	2			
Arbeitsspeicher wird mit gesichert.	1	2	2			
Nutzung von Live-CDs oder Bootsticks, um Beweiskette nicht zu zerstören	3	2	2			
Windows Bordmittel für Ransomware-Schutz wichtiger Ordner	2	2	3			
Role Based Access Control	2	3	3			
Sehr effektiv auch gegen weitere Bedrohungen	4	2	4			
Backups auf read-only setzen	3	1	4			
Offsite-Storage via Internet benötigt eine hohe Bandbreite, auch zur Wiederherstellung!	3	2	3			
	3	3	4			
Hilft bei Prüfung der Recovery Time Objective; notwendige Supportsysteme einbeziehen (z.B. Backup-Server)	3	3	4			
	3	1	2			
Bekannte Malware wird nach einiger Zeit (6 Monate) gebrochen	2	2	2			
	3	4	4			
Nutzen von Blacklists für den „File Server Resource Manager“ automatisiert die Abwehr	2	2	3			
„Kill-Switch“ für Clients, Gefahr von False-Positives	3	2	4			
„Kill-Switch“ für Kommunikation	3	3	4			
Auch an den physischen Zutritt/Zugang zu den Räumlichkeiten denken	3	3	4			
Nutzung des „File Server Resource Manager“	3	3	3			
	1	1	3			
	2	2	2			
	2	2	3			
	2	2	2			
Statistik: Je nach Umfrage zahlen 40-70% der Betroffenen die Lösegeldforderung.						

	Einschätzung VDMA					
Kommentare zu Maßnahmen	**Einrich-tung** 1=geringer Aufwand	**Pflege**	**Nutzen** 5=hoch	**Umsetz-bar?**	**Umge-setzt?**	**Verant-wortlich**
Verhindert das Ausbreiten, aber nicht die Erstinfektion	4	2	4			
Win10: nach BSI-Projekt „SiSyPHuS Win10“	4	3	4			
Mindestens für Tier 0	4	2	3			
Anzahl der Cached Credentials auf „1“ bei Laptops	2	1	2			
schwierig, da hoher Konfigurations- und Pflegeaufwand	4	4	2			
am besten individuelle Zugriffe freischalten	4	3	3			
Microsoft LAPS ist für AD-verwaltete Geräte	3	2	2			
Verbindung zu unbekannten self-signed Zertifikaten unterbinden, lange Liste von Ausnahmen notwendig	3	3	2			
Nutzung von Online-Listen bekannter Server	3	2	2			
Zeit ist Geld. Gerät grundsätzlich eingeschaltet lassen, um forensische Untersuchung zu ermöglichen	2	2	2			
Arbeitsspeicher wird mit gesichert.	1	2	2			
Nutzung von Live-CDs oder Bootsticks, um Beweiskette nicht zu zerstören	3	2	2			
Windows Bordmittel für Ransomware-Schutz wichtiger Ordner	2	2	3			
Role Based Access Control	2	3	3			
Sehr effektiv auch gegen weitere Bedrohungen	4	2	4			
Backups auf read-only setzen	3	1	4			
Offsite-Storage via Internet benötigt eine hohe Bandbreite, auch zur Wiederherstellung!	3	2	3			
	3	3	4			
Hilft bei Prüfung der Recovery Time Objective; notwendige Supportsysteme einbeziehen (z.B. Backup-Server)	3	3	4			
	3	1	2			
Bekannte Malware wird nach einiger Zeit (6 Monate) gebrochen	2	2	2			
	3	4	4			
Nutzen von Blacklists für den „File Server Resource Manager“ automatisiert die Abwehr	2	2	3			
„Kill-Switch“ für Clients, Gefahr von False-Positives	3	2	4			
„Kill-Switch“ für Kommunikation	3	3	4			
Auch an den physischen Zutritt/Zugang zu den Räumlichkeiten denken	3	3	4			
Nutzung des „File Server Resource Manager“	3	3	3			
	1	1	3			
	2	2	2			
	2	2	3			
	2	2	2			
Statistik: Je nach Umfrage zahlen 40-70% der Betroffenen die Lösegeldforderung.						

VDMA
Competence Center Industrial Security
Lyoner Straße 18
60528 Frankfurt am Main

Kontakt
Steffen Zimmermann
Telefon +49 69 6603-1978
E-Mail steffen.zimmermann@vdma.org

industrialsecurity.vdma.org
unternehmen-cybersicherheit.de

DesignStudio