Competence Center Industrial Security

VDMA

VDMA Emergency Guide Ransomware

Content

Introduction

Steffen Zimmermann

The number of ransomware incidents in the mechanical engineering industry increased sharply in recent years. Organizations cannot rely solely on the prevention of cyber attacks – they must assume that sooner or later, they will fall victim to a successful attack. When an attack is successfully executed, the most important element to recovery is to quickly re-establish a stable and secure mode of operation. Small and midsize organizations are particularly at risk; however, they often lack the emergency response policies and crisis management plans required to ensure that appropriate actions are undertaken promptly in the event of a ransomware attack.

This paper from VDMA's Information Security working group provides guidance and answers to fundamental questions pertaining to ransomware infections in addition to a catalogue of measures contact details from independent third parties and generally available information.

Steffen Zimmermann
Head of DMA Competence Center Industrial Security
Secretary of VDMA Working Group Information Security

1 Document Objective and Scope

This document provides assistance and guidance to organizations impacted by a ransomware infection. The document answers the following questions:

1. How can I recognize a ransomware attack?
2. When should I declare a ransomware emergency?
3. What should I do in a ransomware emergency?
4. What should I avoid during and after a ransomware attack?
5. Where can I turn for assistance in the event of a ransomware emergency?
6. What steps can I take to prevent a ransomware attack from occurring or reoccurring?

This document considers potential defensive measures based on a “ransomware kill chain” in the industrial process control industry and makes them available as an overview in an Excel spreadsheet.

This document is intended primarily for IT Managers and IT Security Officers within small and midsize organizations which do not possess adequate internal resources in the area of ransomware risk mitigation and remediation.

This document does not present mandatory requirements for protecting against ransomware attacks - it provides guidance and recommendations underpinned by value-based studies published by independent third parties.

As every ransomware attack is unique, all of the actions and recommendations must be evaluated in alignment with each specific situation.

2 Definition of an Emergency

The German Federal Cyber Security Authority (BSI) defines a ‘general emergency’ as follows:

An emergency is an event in which the processes or resources of an organization do not function as intended. The availability of the corresponding processes or resources cannot be restored in the required time frame. Business operations are seriously impacted. It may be impossible to uphold any existing SLAs (Service Level Agreements). The resulting damages are high to very high and affect the annual results of a company or the ability of a government agency to fulfill its tasks so significantly that such damage is unacceptable. Emergencies cannot be handled during general daily business operations and require a special business and operational continuity response. [BSI 100-4]

Emergencies can also be triggered by disruptions which require an exceptional effort to resolve or that have an unanticipated and/or unforeseeable impact on critical business processes, on customers or on other areas that are of material significance for the organization, such as the loss of data classified as personal data under the GDPR, and thus result in a high level of loss and liability for the organization.

It will be necessary to declare an emergency if defined thresholds are exceeded. Organizations should define these thresholds in advance rather than trying to do so as an incident is unfolding.

3 Ransomware Kill Chain

Even if an organization feels that its IT systems are not secure, it should not regard cyber attacks as spontaneous. Any successful attack requires careful preparation on the part of the attacker. The “Cyber Kill Chain” developed by Lockheed Martin depicts a model attack plan underpinned by sequence of steps, each of which builds on the step before it and each subsequent step which takes an attacker further into the target organization. The VDMA working group has drawn up a ransomware kill chain based on the Cyber Kill Chain. [CyberKillChain]

The ransomware kill chain is used to indicate the points at which appropriate measures could have thwarted the attacker’s advances. The VDMA working group has derived practical measures from the ransomware kill chain model for the email attack vector. Refer to the Excel file for additional details. [VDMA-Excel-Killchain]

The Excel spreadsheet and this document provides possible answers to the question “What now?” that face all impacted organizations at the end of the ransomware kill chain.

Email is just one of many conceivable infection pathways with others including USB keys, service engineers’ PCs, mobile phones, unsecured remote access facilities, unpatched web servers, etc.
The countermeasures required in a particular case may vary from those indicated in the Excel spreadsheet which relate specifically to the email infection pathway.

Case study Ransomware via email

This flow chart describes the classic infection path of ransomware via email. Measures for defense are described in the Excel [VDMA-Excel-Killchain]. Considering and implementing appropriate measures enables you to prevent a further spread of the infection.

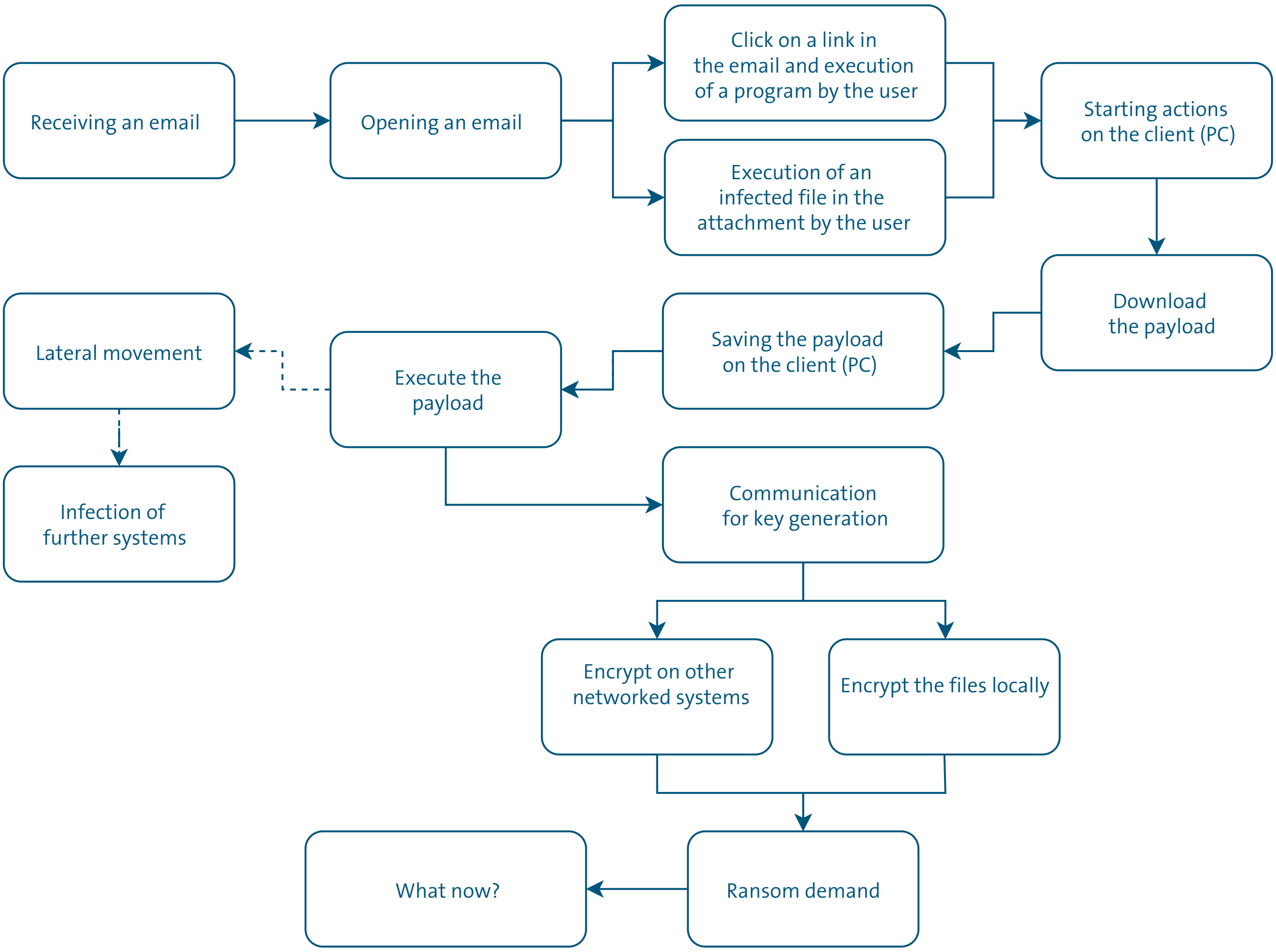
Receiving an email → Opening an email → Click on a link in the email and execution of a program by the user / Execution of an infected file in the attachment by the user → Starting actions on the client (PC) → Download the payload → Saving the payload on the client (PC) → Execute the payload → Lateral movement → Infection of further systems; Execute the payload → Communication for key generation → Encrypt on other networked systems / Encrypt the files locally → Ransom demand → What now?

Figure 1: Ransomware Kill Chain

Source: VDMA

4 How can I recognize a Ransomware Attack?

It is often ordinary employees rather than system administrators who first become aware that there is a cyber-attack in progress. There are a number of typical indicators that can help reveal ransomware incidents.

Common indicators evident to ordinary employees (client PC, file server access)

- PC slows down
- Discovery of encrypted or unreadable files
- Files suddenly become impossible to open
- Unknown files/file extension
- Virus scanner alarm
- Restart in safe mode
- Files containing information/instructions revealing that a hack has taken place (ransom demand)
- Ransom message displayed on screen
- Ransom message on system start-up
- Sudden system restart
- Antivirus software disabled, generates error or does not start
- Instruction to install a program or enter the administrator password
- Sudden change of desktop background
- Emails with unusual or unexpected attachments, links or requests to take unusual actions

The VDMA strongly recommends that organizations provide its employees with cyber security awareness training to help them spot indicators of a cyber attack such as ransomware. The primary objective of this training is to enable employees to better understand what ransomware and phishing emails look like [Phishing] and raise the general level of awareness of these issues and potential deleterious impacts to an organization. The system administrator (IT department) or IT help desk should be contacted immediately if suspicious activities are detected. All employees should be familiar with the relevant emergency contact information which should be available offline so that it can be located in the event of a ransomware attack – as is commonly the case – when accessing an online address book is impossible. Under a cyber attack or ransomware attack, it's important to assume that the telephone system may also be impacted in an emergency.

Common indicators for system administrators

- Typical encrypted files
- Typical file extensions
- Outgoing command and control-traffic at the firewall, IPS or web security gateway
- Blocked emails at the gateway (some may have been delivered)
- Firewall disabled/modified
- All volume shadow copies deleted (fewer copies than usual)
- Internal hosts communicating with external hosts via unusual ports
- Communication and/or alarms at unusual times (outside of normal business hours)
- Suspicious (internal) network scans
- Multiple identical suspicious events occurring at the same time
- Dubious attempts by one user to log in to the network (login attempts from different locations within a short period of time)
- Excessive extension of administrator account authorizations and changes to group policies
- Unauthorized software installations
- Identification and automated deletion of malware at multiple locations simultaneously (this process repeats endlessly)
- Unusual traffic from servers to the internet (domain controllers – http, https, etc.)
- Instances of access to unused shares/files ("canary files")
- Disappearance, failure or incompleteness of backups

A full list of indicators can be found in the detailed Excel spreadsheet. [VDMA-Excel-Indicators]

Important: Indicators may signal a possible attack or ransomware infection to which an expedited reaction is essential. Incident response activities in these circumstances can be a part of daily business process, however, they are not the same as an event that is explicitly declared as an emergency.

5 When should I declare a Ransomware Emergency?

The principle in the context of cyber-attacks is similar to traffic accidents: stay calm and act quickly but deliberately. Ill-considered actions taken in haste could make the situation worse rather than better. Many incidents including the most significant ones can often be resolved without declaring an emergency.

Determination of a ransomware emergency

The following questions can help organizations assess whether a specific instance is actually an emergency. If you answer “yes” to all of them, the situation should be considered a ransomware emergency.

If multiple systems are infected, it should initially be assumed that a large proportion of the network area has been infected or impacted. Where flat network structures without logical or physical protection zones are used, it must be assumed that the entire network is infected. Malware often spreads within a few minutes at current speeds; moreover, encryption often takes no longer than an hour or two given SSDs, Gigabit networks and powerful systems which makes a rapid response critical to minimize damages and impacts.

Damage/loss (effects and spread)

- Is it likely that the infection (encryption) will spread uncontrollably throughout the network?
- Have critical IT systems or information assets become unavailable or are they in acute danger?
- Are critical business processes disrupted or in acute danger?

Time (since when/how much longer?)

- Are the steps to be taken and the time required to resolve the incident unclear?
- Is it likely that it will take an unacceptably long time to restore the processes or systems?
- Is the incident going to have significant deleterious impacts above and beyond internal processes, services and systems (e.g. in the organization’s or customer’s supply chain)?

The following additional questions can help organizations validate a possible ransomware emergency in greater detail:

- Are the attackers still in the process of exploring and taking control of the network?
- Are files still being encrypted?
- Have all files already been encrypted?
- Are privileged accounts affected?
- Can the disruption be contained?
- Can activities be traced in full?
- Are other sites or locations impacted?
- Do you know what steps need to be taken to resolve the disruption?
- Are there backups available of the systems affected?
- Are there any feasible workaround scenarios (mobile communication instead of fixed network, paper instead of PDF, etc.)?
- Have significant areas of production been knocked out?
- Is product quality impacted?
- Is the ability to maintain supply to customers affected?
- Are communication channels compromised?
- Are other non-critical functional areas affected (restaurant, car parks, etc.)?
- Is the disruption having deleterious reputational damages that are apparent to third parties such as the web shop being down and landline communication being suspended?
- Does the disruption meet the criteria for mandatory reporting (to government agencies, business partners, etc.)?

Remark on data protection (acc. to GDPR – European data protection legislation): A breach of the confidentiality of personal data will not necessarily impair the functioning of internal processes; however, it can have significant legal implications in addition to potential reputational damage an organization may face. Any loss of personal data must be formally reported to the respective authorities within 72 hours.

The loss of general but sensitive company data can also trigger an emergency; for example, if sensitive company data ends up with a competitor.

6 What should I do in a ransomware emergency?

The most important thing is to **STAY CALM**.

If there is a risk that an attack, an operating error or a manipulation could harm the functionality or integrity of the IT system, the person who discovers the attack/error/manipulation must take emergency measures independently. In all other cases, the matter must be reported to the IT Manager or IT Support. All activities should be logged with a time stamp and information related to procedure(s) in addition to the person responsible for overseeing resolution. Having a ransomware emergency checklist prepared in advance can help to simplify this documentation process. Technical resources such as file access monitoring, AppLocker and CryptoBlocker are listed in the VDMA Excel spreadsheets.

Protect core systems

- Isolate core systems if possible
- Prevent/restrict user access to business-critical and safety-critical systems

Protect file servers, domain controllers and databases

- Block write access to files for all users (use a script if available)
- Identify the users who have the most files open
- Put file servers into hibernation mode to preserve the device’s working memory

Emergency steps at the device

- NOTE: DO NOT log in to the system with administrator rights if the device is still connected to the network/internet
- Disable the network connection and other communication connections (LAN, Wi-Fi) – if in doubt, deactivate the corresponding ports at the network switch
- Put virtual machines into suspend mode (preserves working memory)
- Put physical machines (PCs) into standby/hibernation mode to preserve the device’s working memory (hibernate mode must first be activated in Windows 10 [Win10])
- Photograph or film ransom demands and relevant events with a smart phone. Record the corresponding device and time along with photos/clips so that they can be assigned correctly at a later time.

Emergency steps on the IT network

- Cut company’s external network connections (firewall, Internet)
- Between all network segments a Src: ANY – Dest: ANY – Service: ANY – Action: “Drop at the top of the firewall ruleset so that network segments can be “started up” one after another during recovery
- Disable network connections to remote sites (MPLS, VPN etc.). If remote sites are already impacted, it may be necessary to configure firewalls to permit only dedicated emergency administration connections (by means of whitelisting) so that malware does not spread uncontrollably to other sites
- Switch off client remote-access
- Switch off internal switches and routers, if it is not possible to isolate network segments (for example floor switches, routers in the manufacturing network)
- Switch off radio networks (guests, staff), for example Wi-Fi, 5G campus network
- Disconnect IT Terminals (laptops, servers, PCs, smart TV, ClickShare, projectors, printers, mass storage devices) from the network

Other emergency steps

- Establish an alternative communication infrastructure (e.g. telephone chain), as attackers may be able to read emails
- Establish an crisis teamm including members from IT, communication, legal and data protection departments
- Do not open or forward any emails or files, even using the cloud, as this could lead to devices outside the network (such as private PCs, customers and suppliers) becoming infected
- Do not log in to either private or company networks from mobile business devices
- Notify branch offices and IT staff at other sites
- Notify external IT service partners (for example cloud service providers) immediately
- Do not attempt unauthorized repairs – always consult a specialist for the systems concerned
- Reinstall affected systems or restore them to a pre-infection state and then back up immediately
- Create clean admin accounts and block all other (admin) accounts
- Stop process rotations (backup rotation, log rotation, snapshot rotation) so that no further data is lost and back up system logs (proxy, firewall, antivirus, Active Directory, VPN, systems affected)
- Redeploy staff which is unable to work due to the incident to other tasks (for example coordination, errands, posting warning notices)

Guidance regarding forensic investigation

The following rules of conduct must be observed so that a forensic investigation can be carried out successfully:

- DO NOT disable the power supply to IT systems
- DO NOT delete any files/systems even if they might be infected with malware
- Create (or initiate creation of) a forensic backup (bitwise 1:1 copy) including a disk image for criminal proceedings
- Avoid installing any software as far as possible and if installation is essential, record the source of the software in addition to the time of installation
- Log every step for every single system from the initial detection of the incident through the completion of the work to resolve it
- Back up relevant log files (antivirus, Citrix, login, firewall, web traffic, etc.) and protect them against manipulation
- Bring in forensic investigation specialists to assist
- If there is a cyber insurance policy in place, contact the insurer's hotline to get support from forensic IT specialists

Establishing of a ransomware emergency management team

Emergency management team

The managing board should appoint/nominate the emergency management team. The primary task of the emergency management team is to ensure business operations are restored as quickly as possible and minimize any consequential damage of an attack.

Members of the emergency management team should include:

- Member of the managing board and stand-in
- Emergency response coordinator and stand-in
- Head of IT / IT Security and stand-in
- Heads of the organizational units affected
- Person responsible for internal/external communication
- Contact person(s) to external service providers whose use is envisaged in emergency situations

Situation room

The members of the emergency management team are notified immediately and meet at a designated location – the situation room – specified by the emergency response coordinator. Information about equipment, admission controls (where applicable) and other security requirements for the situation room is provided in the BSIww standard 100-4 section 7.1.3 [BSI 100-4].

Communication

News of an emergency can rapidly be picked up by the public, media, customers or competitors and judgments can be formed quickly. Communication is therefore one of the main success factors in emergency management. It is necessary to communicate with different stakeholder groups during and after an emergency with the aim of preventing further damage, providing information and avoiding a loss of trust or reputation.

All staff must observe the following requirements:

- Only share comments with the media and external parties through the dedicated communications coordinator
- Avoid conjecture and speculation
- All requests for information must be forwarded to the situation room

De-escalation

- Only the emergency management team has the authority to terminate emergency operations
- The emergency management team notifies all affected organizational units of the plan to return to normal operations
- Any special authorities issued are withdrawn
- The heads of the organizational units submit a status report on the progress of the return to normal operations to the emergency management team at regular intervals
- Once the return to normal operation has been successfully completed in full, the emergency management team disbands

7 What should I avoid?

Typical mistakes in dealing with ransomware attacks include:

Frantic action without deliberation or clear objectives
It is very easy to destroy evidence which can make the subsequent hunt for the perpetrators more difficult. Affected systems cease to pose a threat to other systems once they have been disconnected from the network. Quarantined systems must not be reconnected to the network.

The state of virtual systems can be backed up easily using snapshots (including working memory). Always seek expert support – fear and lack of relevant knowledge can lead to harmful overreaction. Only make use of the expertise of outsiders if you can trust them to maintain strict confidentiality.

Playing down the attack
Ensure that employees at all levels, including the managing board, are notified of the seriousness of the situation. Secrecy only amplifies the negative impact.

Assumptions not facts
Everyone involved should base their decisions solely on facts. Systems are OK? It's a cyber-attack rather than an inside job? Prove it! Use the time to gather evidence and facts.

Uncoordinated actions, individual actions
Coordinate the action plan as a team with the parties directly responsible for the system(s) and make sure to only begin the remediation work once you have a plan; otherwise, you may find that you have to start all over again for no good reason. Different interests work against each other during a security incident. For example,

- Forensic work to secure clues
- Restoration of "functional" data and systems can destroy clues
- External communications
- Confidentiality to be maintained so as not to jeopardize investigations

Continuous coordination of the different tasks is required.

Information outside defined escalation pathways
There must be a single point of contact with customers, employees and the press (where applicable) and this single point of contact must only share information that has been expressly cleared and authorized for release. Proper communication channels must be maintained to ensure that knowledge required for decision-making finds its way to the decision-makers in good time. An excess of information can complicate investigations or provoke further attacks.

Paying the ransom
The statistics show that up to 70% of affected organizations pay the ransom when their business operations fall victim to a ransomware attack. Best practice dictates that paying ransom during a cyber security attack should be avoided at all cost. Paying identifies organizations as an easy target, massively increasing the risk of follow-up attacks; moreover, paying a ransom gives attackers the means to finance subsequent attacks on other victims.

Logging in to infected or insecure systems with extensive authorizations (for example domain admin, local admin with standard password or root)
Many VDMA members who have had this experience found that it was only when the admin logged in that the entire infrastructure became infected. Once a system is infected, it must be assumed that keyloggers, rootkits or token stealing methods have been deployed and that accessing data will immediately be misused to enable the malware to spread to other systems by another pathway.

Connecting unchecked devices to the network
Start with a secure core network to which only verified clean systems are added. Expand the network gradually being careful not to trust any device; be it a laptop, a smart phone, a server or a printer. Use a client firewall by default to limit incoming connections to "need to access" only.

Use of hastily downloaded "rescue tools" (secondary infection)
Only use tools that have been downloaded from trusted PCs or servers and that originate from trusted partner sources such as from your antivirus vendor or Microsoft; otherwise, organizations may end up with a new infection on the last remaining clean devices.

The deleting encrypted files in haste
Websites https://www.nomoreransom.org and https://id-ransomware.malwarehunterteam.com/index.php?lang=en_US enable access to decryption tools for older ransomware. In some cases, there may be a way to recover or restore availability within an acceptable period of time without paying any ransom.

Switching off infected computers (but infected computers must be disconnected from the network - incl. WiFi!)
There is a possibility that technical experts might still be able to identify the encryption mechanism or infection pathway stored within the RAM.

Hasty upload of files to cloud services (for example VirusTotal, Hybrid Analysis)
Uploading files can represent an information leak because these files could be accessible by the partners of the service providers. Only upload files that do not contain company, commercial secrets or personal data. Where applicable, calculate the hash value of the files and request the hash value from the service provider.

Overly hasty restarting of infrastructure
Do not restart the systems too quickly. There's no question that management will be keen to get systems and operations back online as quickly as possible; however, the risk of re-infection remains very high until every last system has been checked and cleared. Experience with infections in the mechanical engineering industry indicates that in the event of a comprehensive ransomware infection, a wait of four to six weeks before the production systems can be restarted is not unusual. Complete processing of the incident from the perspective of the IT function generally takes six to nine months. From the perspective of business administration, it is necessary to plan for high financial impacts and expenditures for a number of years following a ransomware incident.

8 Where can I turn for assistance in an emergency situation?

Initial assistance with ransomware incidents can be obtained from government agencies, specialist communities in addition to security consulting companies. A condensed list of current contact addresses can be found in the annex of this paper.

Government agencies
German-speaking government agencies are currently only able to provide a limited amount of emergency assistance in relation to ransomware and what they offer is intended primarily for infrastructure operators whose services are considered to be critically important for the public (Critical Infrastructure Protection, "KRITIS").

The following government agencies may be able to support during a ransomware incident:

- German Federal Office for Information Security (BSI)
- Central points of contact for cybercrime (Zentrale Ansprechstellen Cybercrime, "ZAC") at the Criminal Police Offices of the German states
- Local specialist police departments for cybercrime, where available
- MELANI Reporting and Analysis Centre for Information Assurance (Switzerland)
- "Against Cybercrime" reporting system (Austria)
- Europol maintains a list of Cybercime reporting websites which can serve as a first line of contact.

The state of Baden-Württemberg's ZAC has its own specialist digital investigative unit; the "Task Force Digitale Spuren". Not all of the ZAC are as well-prepared for ransomware emergencies. Contact details for the government agencies are provided in the annex of this paper for easy reference.

Certain areas of cyber security attacks can only be investigated by the public prosecutor's office; as such, it is advisable to submit a report promptly and collaborate closely with the public prosecutor's office.

Specialist communities/cyber security initiatives
Specialist communities can be a useful first point of contact and may be able to refer organizations to partner companies in the private sector.

- Alliance for Cyber Security (Allianz für Cyber-Sicherheit, "ACS"): qualified service provider for APT response
- Cyberwehr BW: emergency assistance for companies in the state of Baden-Württemberg

Consulting companies
Many consulting organizations have dedicated IT security specialists. Specialists in the area of rapid emergency assistance in ransomware cases (including VDMA members and APT service providers accredited by the German Federal Office for Information Security) are listed in the annex of this paper.

9 What steps can I take to prevent it from happening (again)?

Your response to a ransomware incident should involve more than just emergency measures because you certainly do not want to go back to using the very same information technology as prior to the attack. It is therefore very important that organizations incorporate the “right” (i.e. better and stronger) security measures when re-establishing the infrastructure: lessons learned. All of the measures listed below are also considered ideal preventive measures.

Generic measures for immediate implementation

The VDMA working group advises organizations to review and implement the following basic measures irrespective of the attack vector:

- Avoid and disable direct remote administration access to internal IT systems, particularly RDP, Citrix and SSH
- Two-Factor Authentication (2FA) for systems that are accessible from the Internet
- Deactivation of SMBv1 on all systems
- Patch management for operating systems and applications (i.e. PDF Reader, Office, image editing, etc.)

Measures have been derived in alignment to the email attack vector (ransomware kill chain) that would have mitigated the infection chain at specific points. The full list of measures can be found in the Excel spreadsheet [VDMA-Excel-Killchain].

The VDMA working group considers the following selected measures to be so important that it suggests making their implementation a mandatory requirement:

- Awareness training
- Flagging of external emails
- Restriction of user rights
- Policy for admin accounts (with Microsoft LAPS where applicable)
- Blocking of potentially hazardous file types
- Disabling of Microsoft Office macros
- Network segmentation
- Limitation of incoming connections to clients
- Isolation of vulnerable legacy systems (own network zone, dedicated admin group)
- Internet access limited to via proxy server (with threat protection)
- Limitation of remote access - no direct access via RDP, Citrix
- Blocking of network traffic to/from the TOR network (both directions)
- Regular backups and off-site storage of backup media
- Checking that critical systems can be restored in full
- Development of kill switches for communication connections

Additional measures

If permanent protection is to be provided with all risks minimized, it is necessary to identify the organization’s specific risks in a structured manner and to implement coordinated measures defined on the basis of the results. This involves minimizing or avoiding risks and transferring them (with insurance, for example) or knowingly accepting them.

Complete security checklists

Basic checklists can help organizations to focus on their efforts in the right areas. Comparisons with organizations of similar size or in the same industry sector can play an important role to focus on in this process. We recommend that organizations use the Heise Security Consulter for this activity: https://www.heise-consulter.de/. The result will be a comparison appropriate for the organization’s specific situation.

IT security protection policy as specified by the German Federal Office for Information Security (BSI)
More sustainable than deriving individual measures (“filling in the gaps”) is a comprehensive IT security policy in accordance with the BSI’s baseline IT protection methodology (“IT-Grundschutz”) which also includes an emergency preparedness module. The baseline protection methodology, which has proven popular with small and midsize organizations in the process control industry, is available free of charge. It also includes a module for industrial control systems that covers the special features of manufacturing companies. A digital training course on the implementation of management measures, which was prepared jointly with VDMA members, can be found on the University4Industry [U4I] website.

Draw up (and verify) an emergency plan
There is no such thing as perfect security. Organizations should proceed on the basis that the possibility of an attack succeeding will never go away and that their entire infrastructure is likely to be taken down (again) at some point in the future. Create an emergency policy to prepare for this event. The VSMA has created a model emergency plan for cyber-attacks based on the BSI’s emergency management (100-4) module. Organizations should leverage this model to prepare their own comprehensive plan for an emergency. [VSMA]

The VSMA provides access to this and other aids from the VDMA and VSMA at https://unternehmen-cybersicherheit.de.

The BSI’s IT emergency card (“IT-Notfallkarte”) provides a useful model for a notice to display on site so that employees have quick access to information about reporting pathways and basic measures in the event of a new IT emergency. [BSI-Notfall]

Check cyber insurance
While an insurance policy can do no more than offset the losses incurred in a cyber security incident, all insurers offer the option to consult with named experts in the field regarding the improvement of cyber defense strategies and best practices. Insurance companies can also put policyholders in contact with emergency/forensic investigation service providers or arrange associated services in connection with a cyber insurance policy. The VDMA cyber policy [VCP] provides an insurance framework tailored to the requirements of manufacturing companies. The Information Security working group has examined the suitability of the VCP in 16 typical scenarios together with the VSMA. The scenarios and the VSMA’s assessment can be requested free of charge from the VDMA or VSMA. [VCP-16]

Additional links to sources of help and templates/model documents are presented in the next section.

10 Additional information and sources

An overview of additional sources of information relating to ransomware and incident response is provided below.

Prevention

[VDMA-Excel-Killchain]	VDMA ransomware kill chain – infection via email
[VDMA-Excel-Indicators]	VDMA indicators of a possible ransomware infection
[VSMA]	Model IT/cyber emergency plan
	VDMA CyberPolice (VCP)
[VCP]	VDMA cyber policy
[VCP-16]	16 attack scenarios and coverage in the VDMA cyber policy (available via Biljana.Gabric@vdma.org)
[BSI]	Protecting against ransomware 2.0
[BSI 100-4]	BSI Standard 100-4: Emergency Management
[IHK]	IHK guidelines for IT emergencies
[NIST]	NIST Computer SecurityIncident Handling Guide
[GOVCERT]	GOVCERT Ransomware Countermeasures (en)
[CryptoBlocker]	CyptoBlocker for ransomware file types on Windows file servers
[PowerShell]	PowerShell Security Best Practices
[AppLocker]	Windows AppLocker from Microsoft
[Phishing]	Information from the German citizens' advice network Verbraucherzentrale about Emotet
[U4I]	Online industrial security management training course
[CyberKillChain]	Lockheed Martin Cyber Kill Chain
[ProcessBouncer]	Proof of concept for ProcessBouncer by Holger Junker (BSI)

Simulation

[KnowB4]	KnowB4 software for simulating a ransomware attack
[CyberReliant]	Ransomware kill chain

Response

[Win10]	Enabling hibernate mode in Windows 10
[BSI-Ersthilfe]	Initial assistance in response to a serious IT security incident
[BSI-Notfall]	IT emergency card
[aramido.de]	Ransomware crisis management plan
[NoMoreRansom]	No More Ransom – decryption tools
[CyberWehr]	https://cyberwehr-bw.de/ cyber defense for companies in Baden-Württemberg

11 Editorial team

From the sector for the sector. Colleagues from the VDMA's Information Security working group are actively working on documents suitable for practical use. The working group is also attending to assessments on current matters, investigating topics for the future and using the network of IT security officers within the VDMA for informal experience sharing.

Active authors

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 Städinger
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 Information Security working group

Chairman: Rolf Strehle, Voith

VDMA e. V.
Abteilung Informatik
Lyoner Str. 18
60528 Frankfurt/Main, Germany

translated: 2021-03-01

12 Annex: Contact points

Government agencies

The central points of contact for cybercrime (Zentrale Ansprechstellen Cybercrime, “ZAC”) are in principle the first point of governmental contact. If your state ZAC is unable to help, you can request help from the German Federal Criminal Police Office (BKA) or German Federal Office for Information Security’s Computer Information Security’s Computer Emergency response Team for federal agencies (“CERT Bund”) as an alternative. Unfortunately, the reporting systems for cybercrime in Austria and Switzerland do not provide telephone numbers for use in an emergency. Additionally, the resources from BKA and BSI are solely in German only. An overview of cybercrime resources in Europe can be obtained by Europol.

State/country	Telephone number	Email address
Europe (Overview)	[none]	https://www.europol.europa.eu/report-a-crime
MELANI (Switzerland)	[none]	https://www.ncsc.admin.ch/ncsc/en/home.html
Reporting system (Austria)	[none]	against-cybercrime@bmi.gv.at
BSI CERT Bund	+49 (0)228 99 9582 222	certbund@bsi.bund.de
German Federal Criminal Police Office (“BKA”)	0611 55-15037	zac@cyber.bka.de
Baden-Württemberg	+49 (0)711 5401-2444	cybercrime@polizei.bwl.de
Bavaria	+49 (0)89 1212-3300	zac@polizei.bayern.de
Berlin	+49 (0)30 4664-924924	zac@polizei.berlin.de
Brandenburg	+49 (0)3334 388-8686	zac@polizei.brandenburg.de
Bremen	+49 (0)421 362-19820	cybercrime@polizei.bremen.de
Hamburg	+49 (0)40 4286-75455	zac@polizei.hamburg.de
Hessen	+49 (0)611 83-8377	zac.hlka@polizei.hessen.de
Mecklenburg-Vorpommern	+49 (0)3866 64-4545	cybercrime.lka@polmv.de
Lower Saxony	+49 (0)511 26262-3804	zac@lka.polizei.niedersachsen.de
North Rhine-Westphalia	+49 (0)211 939-4040	cybercrime.lka@polizei.nrw.de
Rhineland-Palatinate	+49 (0)6131 65-2565	lka.cybercrime@polizei.rlp.de
Saarland	+49 (0)681 962-2448	cybercrime@polizei.slpol.de
Saxony	+49 (0)351 855 - 3226	zac.lka@polizei.sachsen.de
Saxony-Anhalt	+49 (0)391 250-2244	zac.lka@polizei.sachsen-anhalt.de
Schleswig-Holstein	+49 (0)431 160-4545	cybercrime@polizei.landsh.de
Thuringia	+49 (0)361 341-4545	cybercrime.lka@polizei.thueringen.de

The current list of contact points in Germany can be found here: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Meldestelle/Polizeikontakt/ZACkontakt/zackontakt.html

VDMA member contact points

The following member companies of the VDMA Software and Digitalization trade association already have experience of dealing with ransomware emergencies in the mechanical engineering industry.

Company	Location	Contact information	Emergency number*
@-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

*Available 8 a.m. - 5 p.m. unless otherwise indicated

Companies accredited by the BSI for APT attacks

According to the German Act on the Federal Office for Information Technology (“BSIG”), the BSI is charged with advising and supporting operators of critical infrastructures in their efforts to secure their information technology. This can include referring infrastructure operators to qualified providers of security services. The following companies have completed the qualification process to achieve accreditation as an APT Response Service Provider:

The APT Response Service Providers have been accredited by the BSI using transparent criteria and processes. These include a comparison of specific performance features of the service providers as well as the publication of contact details. The BSI document containing the selection criteria, performance features and comparison can be found at

https://www.bsi.bund.de/EN/Home/home_node.html

Company	Emergency contact	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

(Last revised: December 2019)

Ransomware indicators

Last revised: 2020-01-28 • © VDMA e.V.

		On what drive?			Detection	
Indicators	**Can be automated?**	**Client**	**File server (Explorer)**	**Server (OS)**	**User**	**Power User**
Computer slows down		x		x	x	x
Encrypted files detected	x	x	x	x	x	x
Files suddenly become impossible to open		x	x	x	x	x
Unknown files	x	x	x	x	x	x
Files containing information/instructions revealing that a hack has taken place (ransom demand)		x	x	x	x	x
Unknown new processes in Task-Manager		x		x		x
Unknown new user in Task-Manager		x		x		x
Autostart entries	x	x		x		x
Registry run entries	x	x		x		x
Services		x		x		x
Virus scanner alarm	x	x		x	x	x
Outgoing C2 traffic at firewall	x	x		x		
Access to odd/unknown URLs	x	x		x		
Information from staff member that he/she clicked		x			x	x
Blocked emails at the gateway (some may have been delivered)	x			x		
Ransom message displayed on screen		x		x	x	x
Ransom message on boot		x		x	x	x
Sudden system restart?		x		x	x	x
Anti-virus-software disabled/generates error and does not start	x	x		x	x	x
Instruction to install a program or enter the administrator password		x		x	x	x
Change to the desktop background		x		x	x	x
Emails with unusual or unexpected attachments, links or requests to take unusual actions	x	x			x	x
IDS events	x	x		x		
SIEM events	x	x		x		
Firewall disabled/modified	x	x		x	x	x
Anti-virus-software disabled/generates error and does not start		x		x	x	x
All volume shadow copies deleted (far fewer than usual)	x			x		
Internal hosts communicating with malicious or unknown target addresses	x	x		x		
Internal hosts communicating with external hosts via unusual ports	x	x		x		
Communication and/or alarms at unusual times (compared to normal business hours)	x			x		
Publicly accessible hosts or hosts in demilitarized zones (DMZ) communicating with internal hosts	x			x		
Suspicious (internal) network scans	x	x		x		
Multiple identical suspicious events occurring at the same time	x	x	x	x	x	x
Rapid reinfection with malware after resolution can indicate the presence of a rootkit or incomplete elimination (for example dropper not detected)		x		x		
Dubious attempts by one user to log in to the network (login attempts from different locations within a short period of time)	x			x		
Excessive extension of administrator account authorizations and changes to group policies	x	x		x		
Unauthorized software installations	x	x		x		
Access to canary files/shares	x	x	x	x		
Sudden increase in activity on NAS resources from multiple systems	x			x		
Disappearance, failure or incompleteness of backups	x		x	x		
Identification and automated deletion of malware at multiple locations simultaneously (this process repeats endlessly)	x	x	x	x		
Unusual traffic from servers to the internet (domain controllers – http, https etc.)	x			x		

Time window since initial infection		Applicability			
Manual	**Automated**	**Awareness**	**IoC script**	**Avoidable?**	**Recommended**
"Minutes (during business hours)"	-	x			
"Minutes (during business hours)"	Seconds	x	x	x	"Client: enable Windows ransomware protection File server: enable FSRM, block user [fsrm] [cryptoblocker]"
"Minutes (during business hours)"	-	x			
"Minutes (during business hours)"	Seconds	x	x	x	"Activate and configure FSRM [fsrm] [cryptoblocker]; Use file extension list [fel]"
"Minutes (during business hours)"		x			
Forensic investigation				x	Application whitelisting using AppLocker [applocker]
Forensic investigation					
Forensic investigation	Seconds		x		
Forensic investigation	Seconds		x		
Forensic investigation					
hours	Seconds	x	x		
Forensic investigation	Seconds		x	x	"Use of C2 lists of known server Ips [C2-List] Surfing only via web proxy, avoid direct internet connection; web access from servers severely restricted (for example Windows Update only)"
Forensic investigation	Seconds		x	x	Surfing only via web proxy, avoid direct internet connection; web access from servers severely restricted (for example Windows Update only)
"Minutes (during business hours)"		x			
Forensic investigation	Seconds		x		
"Minutes (during business hours)"		x			
"Minutes (during business hours)"		x			
"Minutes (during business hours)"		x			
"Minutes (during business hours)"	Seconds	x			
"Minutes (during business hours)"		x			
"Minutes (during business hours)"		x			Can also be caused by energy saving settings (false positive)
"Minutes (during business hours)"		x	x	x	Mitigation using file filter, also with Microsoft Power Automate (Flow)
Forensic investigation	Seconds		x		
Forensic investigation	Seconds		x		
Forensic investigation	Seconds		x		
"Minutes (during business hours)"		x	x		
Forensic investigation	Seconds		x	x	vssadmin.exe disabled via AppLocker [vssadmin]
-	Minutes		x	x	Surfing only via web proxy, avoid direct internet connection; web access from servers severely restricted (for example Windows Update only)
-	Seconds		x	x	Prevent at the firewall, automated lockdown
-	Minutes		x		Dependent on the company's business area
-	Seconds		x	x	Prevent at the firewall
-	Seconds		x	x	Prevent at the firewall, automated lockdown
"Minutes (during business hours)"	Minutes	x	x		IT support should be prepared to pick up on potential correlations of events
hours					
Forensic investigation	Minutes		x	x	Automated time-dependent lock-down of a user account
Forensic investigation	Seconds		x		
Forensic investigation	Seconds		x	x	Application whitelisting using AppLocker [applocker]
Forensic investigation	Seconds		x		
Forensic investigation	Seconds		x		
days	Seconds		x	x	Provide for backup and restore using specific accounts and authorizations, use FSRM to identify deletion/modification of backups
Forensic investigation	Seconds		x		
Forensic investigation	Minutes		x		Anomaly detection

Ransomware-Kill-Chain

Last revised: 2020-01-210 • Use Case: Attack via email • © VDMA e.V.

Principal assumptions

No blame attaches to the uninformed user/The network cannot be switched off/Ransomware attacks work on fully patched systems/ Protection can only be realized with graduated measures

Attack steps	Risks	Manda-tory?	Measures
Receipt of an email	R: Sender faked		M: DNS & IP tools: Use of SPF, DKIM, DMARC, email-blacklists, Spamcop etc.
			M: DNAE Domain Named Authenticated Entities
			M: Restriction of "spam authenticity" (counterfeit emails can look very realistic)
		yes	M: Awareness training: Do not rely on easily falsified display names
		yes	Flagging of external email as "External"
	R: Email with executable file as attachment	yes	M: Block hazardous file types – executable files at least
	R: Email with active content in the attachment (Office for example)		M: Restriction of receiving rights to specific groups
			M: Remove macros in Office files automatically on receipt
			M: Implement BSI recommendation concerning group policies for Microsoft Office
			M: Allow signed macros only (or a more restrictive policy) in Office
Opening an email	R: Opening of a private email via webmail		M: Make users aware of the risk; organizational guideline
	R: The attachment contains an executable file		M: Restrict receipt of executable files
Execution of a scripted file by the user	R: Works on fully patched systems because the file is executed by the user		M: Use antivirus program heuristics/"AI"
			M: Behavior-based analysis/defense
			M: Sandboxing (gateway)
		yes	M: Disabling of Office macros via group policy; enabled only for selected users
Starting of actions on the client	R: User has comprehensive rights	yes	M: No user logged in has admin rights
Downloading of the payload	R: Download in the background not visible	yes	M: Internet access only via proxy or NGFW with Deep Packet Inspection
	R: Executable file download		M: Executable files downloadable only after confirmation of a dialog
		yes	M: Block downloading of executable files
	R: Download of specific payload pages		M: Block unneeded IP address ranges
			M: Block unneeded DNS ranges (?)
		yes	M: Block TOR network
		yes	M: Install blacklists for known IOC (for example Emotet) if system/proxy in place
	R: Downloading of specific malware	yes	M: Blocking of known file types
			M: Monitoring of network activities, for example with SIEM
			M: Activation of sandbox method in web filter
			M: Detection and blocking by virus scanner with intrusion prevention
Saving of the payload on the client	R: Saving of undetected malware		M: Application directory whitelisting (disable write authorizations)
Execution of the payload	R: Execution of malware		M: Application whitelisting
	R: Execution of files in certain folders		M: Restrict Temp folders using AppLocker/software restriction policies
		yes	M: Enable protected view for Office documents in Temp and Download folders
	R: User has admin rights		M: Transfer admin rights to a dedicated account
		yes	M: Daily working but without admin rights
	M: Restrict communication capabilities in local firewall		M: Restrict SMB/SMTP/etc. communication to approved applications

Measures to be implemented irrespective of attack vector (not email specific)
Avoidance of direct remote administration access to internal IT systems (for example RDP, Citrix, SSH etc.)/Deactivation of SMBv1 on all systems/
Patch management for operating systems and applications (for example PDF Reader, Office etc.)

	VDMA assessment					
	Configuration	**Maintenance**	**Use**	**Feasible?**	**Implemented?**	**Responsible**
Comments regarding measures	1=simple		5= complex			
Blacklists must be updated regularly and it should be possible to define exceptions for customers	4	2	5			
Certificate check by sender	4	2	3			
Configure mail server so that SPAM is readily identifiable for users	2	2	3			
Permanent protection requires repetition as well as training new staff	5	3	4			
Reluctance among sales staff	1	1	3			
https://www.govcert.ch/downloads/blocked-filetypes.txt	1	1	3			
Risk of status becoming permanent for all staff	3	2	2			
Difficult to implement, defective files possible	5	1	2			
Very complex	4	3	4			
Standard setting in Office	1	1	3			
Possibly also restrict automatically using web filter	2	2	2			
	1	1	3			
Statistics: 10 % of users typically click on a phishing email	2	2	3			
Usually integrated in the case of next-generation AV	2	2	3			
Attackers can detect sandboxing	3	3	3			
Reluctance among of staff, as a large amount of home-spun in circulation	1	3	3			
Spread limited to systems with write authorizations	2	1	4			
Proxy server can simultaneously check file content – https traffic interception	3	3	3			
Raises awareness, proxy or web filter required	3	3	2			
Exceptions are very burdensome for the IT department	2	4	3			
Block also helps against other attacks, should additionally be made dynamic	2	2	3			
Block alternative DNS servers	2	1	2			
Could block regular communication	3	2	2			
	2	2	3			
Exceptions are burdensome for the IT department	2	2	3			
Evaluation has to be planned	4	3	4			
Attackers can detect sandboxing	2	2	3			
Usually integrated in the case of next-generation AV	2	2	3			
Additional monitoring for encryption with standard Windows tools	3	3	4			
Difficult, as substantial effort required for configuration and maintenance; only recommended for non-patchable or stable systems	3	3	4			
Difficult, as substantial effort required for configuration and maintenance; only recommended for non-patchable or stable systems	3	3	3			
Does not prevent automatic execution	1	1	2			
Does not prevent execution of the harmful code	3	3	3			
	3	3	3			
Prevents spread but not initial infection	3	2	3			

Ransomware-Kill-Chain

Last revised: 2020-01-210 • Use Case: Attack via email • © VDMA e.V.

Attack steps	Risks	Mandatory?	Measures
Spread/lateral movement	R: Use of (un)known and unpatched vulnerabilities		M: Regular installation of security updates
			M: Implement basic system hardening measures
			M: Implement Microsoft Tier Model for the AD architecture
	R: Attacker gains privileges with admin login		M: Disablement of WDigest caching, credential caching, etc.
			M: Restriction of inherited/delegated authorizations
			M: Prohibit "privileged accounts" from accessing other security zones (clients, servers, domains).
			M: M: Use of a dedicated account for local administration (for example LAPS) instead of one general account for all devices
Communication regarding key regeneration	R: Encrypted communication with C2 server		M: Enable proxy login with certificate check
			M: Prevent communication with known C2 servers
Encryption of files locally	R: All files are encrypted locally		M: Remove clients from the network
			M: Pause virtual machines or create snapshot with memory
			M: Forensic backup of the computer affected
			M: Checking of key folders for suspicious activities
Remote encryption	R: Access with the user's rights	yes	M: Restrict write authorizations
		yes	M: Segment network to prevent access to other systems
	R: Important data is encrypted	yes	M: Regular system backups
		yes	M: Offsite storage of backups; storage at a different location
			M: Backup testing (regularly)
		yes	M: Checking that critical systems can be restored in full
			M: Identification of patient zero
			M: Retention of encrypted files
			M: Monitoring of network activities with SIEM
			M: Install scripts for the detection of ransomware file extensions and access to canary files/shares
			M: Install scripts to block hazardous clients on detection
	Define measures to be implemented immediately	yes	M: Prepare deactivation of connections to other locations
			M: Delegate authority to disconnect network components to local managers
			M: Prepare script to disable write authorizations for storage systems automatically
Ransom demand			M: Screenshot
			M: File official report
			M: Seek assistance of/notify state Criminal Police Office ZACs
			M: Convene BSI situation room team
Payment			M: There is no way to be sure that data will actually be released on payment of a ransom, so we advise against making any payment.

	VDMA assessment					
	Configuration	Maintenance	Use	Feasible?	Implemented?	Responsible
Comments regarding measures	1=simple		5= complex			
Prevents spread but not initial infection	4	2	4			
Win10: Per BSI project "SiSyPHuS Win10"	4	3	4			
At least for tier 0	4	2	3			
Number of cached credentials on laptops set to "1"	2	1	2			
Difficult, as substantial effort required for configuration and maintenance	4	4	2			
The best option is to approve access at the individual level	4	3	3			
Microsoft LAPS is for AD-administered devices	3	2	2			
Prevention of connection to unknown self-signed certificates, long list of exceptions required	3	3	2			
Use of online lists of known servers	3	2	2			
Time is money. Leave device switched on (in principle) to facilitate forensic investigation	2	2	2			
Working memory is also backed up.	1	2	2			
Use of live CDs or bootsticks to avoid destroying the chain of evidence	3	2	2			
Standard Windows tools for ransomware protection of important folders	2	2	3			
Role-based access control	2	3	3			
Also very effective against various other threats	4	2	4			
Set backups to read only	3	1	4			
Offsite storage via the internet requires high bandwidth, including for restoration	3	2	3			
	3	3	4			
Helps when checking the recovery time objective; include necessary support systems (for example backup servers)	3	3	4			
	3	1	2			
Known malware will be cracked after a certain period of time (six months)	2	2	2			
	3	4	4			
Use of blacklists for the File Server Resource Manager automates defense	2	2	3			
Kill switch for clients, risk of false positives	3	2	4			
Kill switch for communication	3	3	4			
Remember also to consider physical access/admission to premises	3	3	4			
Use of File Server Resource Manager	3	3	3			
	1	1	3			
	2	2	2			
	2	2	3			
	2	2	2			
Statistics: surveys report that between 40 % and 70 % of affected parties pay the ransom.						

VDMA
Competence Center Industrial Security
Lyoner Str. 18
60528 Frankfurt am Main

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

vdma.org/cybersecurity
unternehmen-cybersicherheit.de

Picture: Shutterstock
DesignStudio