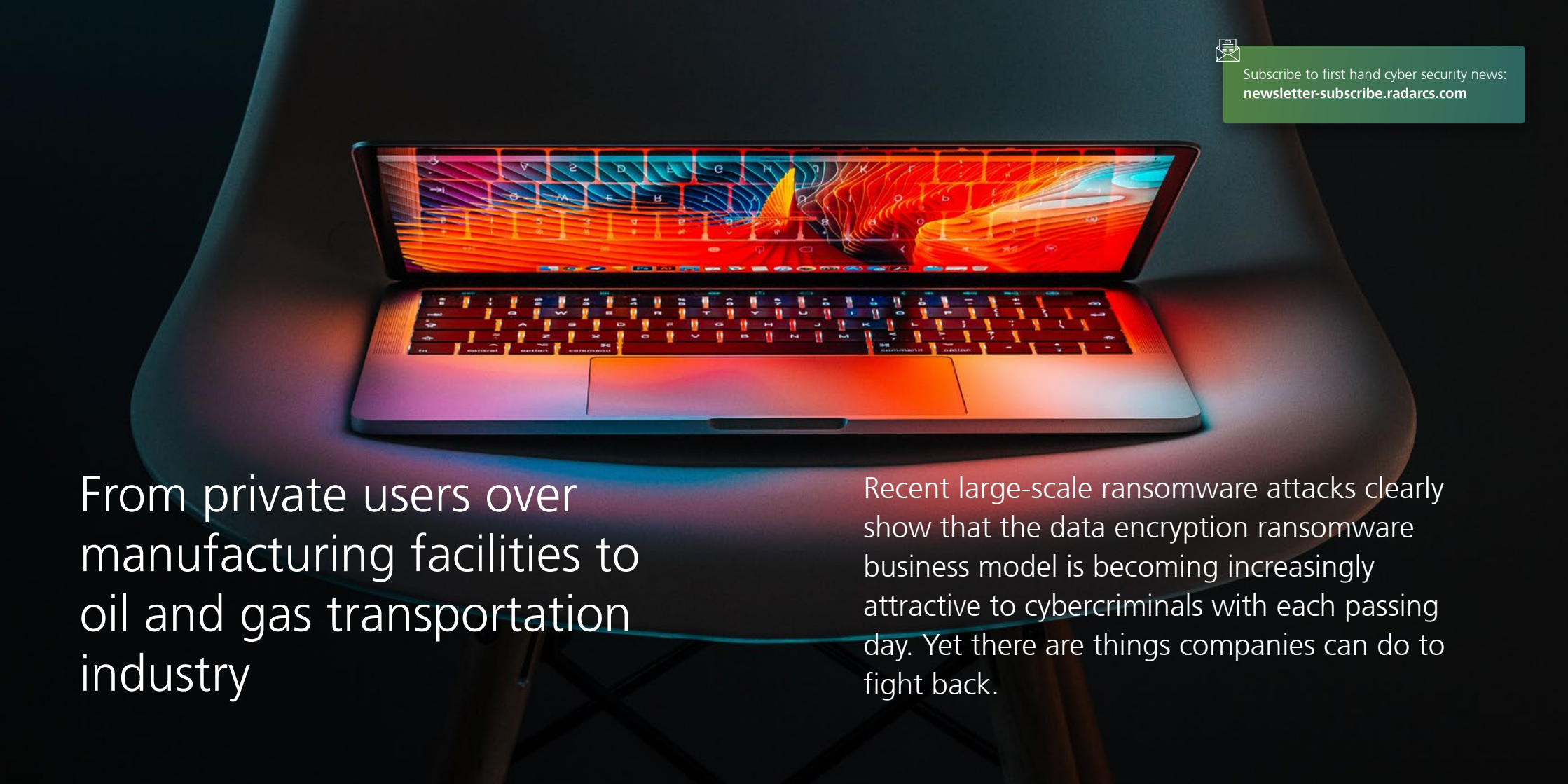

RADAR
CYBER SECURITY
RANSOMWARE GUIDE
Fighting ransomware
Key measures in the battle against ransomware using data encryption



From private users over manufacturing facilities to oil and gas transportation industry

Recent large-scale ransomware attacks clearly show that the data encryption ransomware business model is becoming increasingly attractive to cybercriminals with each passing day. Yet there are things companies can do to fight back.

Why is the number of ransomware attacks rising?

"Companies that are ready cannot be extorted. They detect and stop ransomware before any important data are lost."

— Lothar Hänsler, COO, Radar Cyber Security

Let's start with some basics

Ransomware is a form of extortion software that encrypts its victims' data or blocks access to entire computer systems. The attackers often threaten victims with data encryption if the ransom is not transferred in time (commonly cryptocurrency). Today's advanced ransomware is often designed to spread like a virus throughout a network, targeting database and file servers. If the attack succeeds, it has a serious impact on business processes and can quickly force an entire company to its knees. In many cases organizations have a hard time dealing with the technical consequences for months, as well as the effects on their businesses for years.

Cybercriminals have also honed their ransomware tactics over time, adding a second layer of extortionist behavior, by threatening their victims to make the stolen data public if they refuse to pay.

Easy money in no time

Unfortunately one must admit: creating ransomware is not a rocket science. Cryptotrojan attacks have become a convenient and lucrative weapon in the arsenal of even the most technologically challenged criminals thanks to the professionalism of distribution channels such as Ransomware-as-a-Service. The dark net is packed with ransomware marketplaces offering malware strains for every cybercrime-wannabe. Ransomware-as-a-Service platforms enable novices to enter the cyberextortion business without risk and to obtain the corresponding service from malware developers in exchange for a fee or commission. The question is therefore not if a company will be attacked with ransomware, but when.

Ransomware is a business-vital challenge

Experienced criminals do not act like someone holding up a gas station, grabbing the contents of the cash register once and fleeing. They are biding time. Sophisticated attacks often last several months, from the time the IT system is first infiltrated to the moment when extortion begins. Cybercriminals wait for the right moment for causing the maximum inconvenience: prior supervisory board meeting, general meeting of shareholders, signing a major customer contract or a strategic partnership. Time and decision-making pressure make company management more susceptible to extortion. Being highly resilient to cyberattacks has long since ceased to be the sole responsibility of the IT department, being instead a strategic issue with which management ensures its ability to act.

To pay or not to pay?

Given the length of time needed to recover from such an attack, managers of affected companies normally consider acquiescing to the cybercriminals' demand. Managers need to consider in advance whether a company will pay the ransom or not instead of making a snap decision in the heat of the moment.

In doing so, they should be aware of the disadvantages of paying: firstly, there is no guarantee that the crime actors will actually hand over the decryption key. In a worst case scenario, the target company will have to rebuild its systems from scratch despite having paid a ransom. Secondly, even if the key is obtained, it often happens that some data are damaged and cannot be repaired. Thirdly, complying with the demand for payment makes any company a particularly attractive target for follow-up attacks. Thus the key here is to develop cyber resilience that works regardless of who is trying to attack.

Let alone the term ransomware can lead decisionmakers to make the wrong conclusions, alongside following the motto "If we pay, the problem is gone". This misconception ignores the fact that a successful ransomware attack highlights just how fragile the IT infrastructure is and that ransom itself may not necessarily be the attackers' only or primary goal. More often than not, it is simply a smoke screen. In the worst case, companies pay the ransom and yet disappear from the market shortly afterwards because their highly sophisticated products are suddenly being copy-manufactured in the Far East in an identical way using the original outlines.

All this means that when considering their approach in the battle against ransomware, companies should always bear the following points in mind: "How can I protect IT infrastructure from getting penetrated and, if necessary, how to stop it as quick as possible?" and "How can we guarantee our business continuity at all times?"

How to ensure business continuity

What can companies do to ensure that their underlying business operations cannot be undermined by attacks? These are three core recommendations to consider:

"Cybersecurity is so much more than traditional IT. It is a strategic business issue and directly linked to business continuity. Companies that target this are treating the issue the same way they treat Human Resources or R&D at board level."

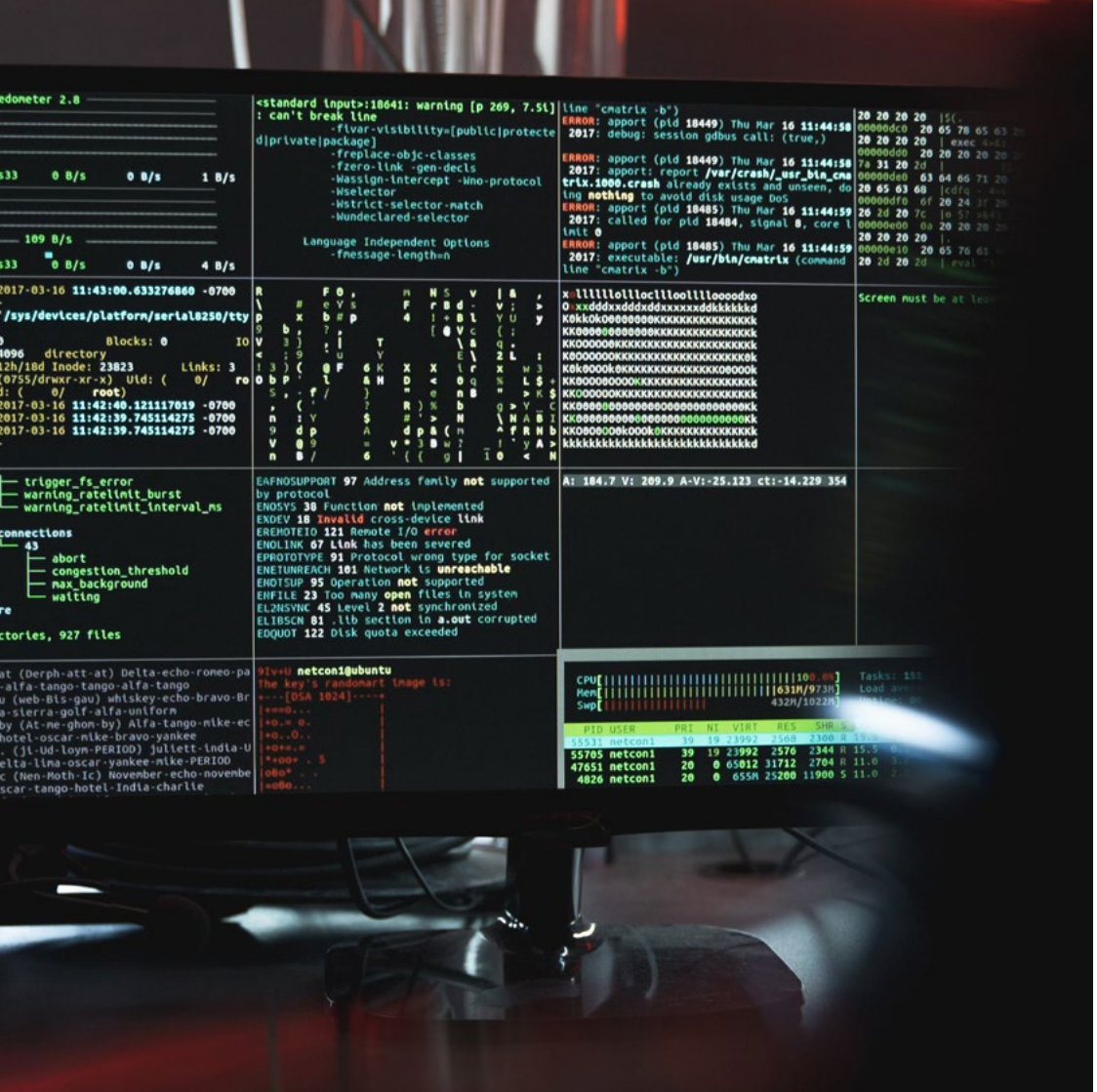
— Ali Carl Gülerman, CEO, Radar Cyber Security

1 Identifying corporate jewels

What are your most important company assets? It does not matter whether these are intellectual property, trade secrets or customer data, these are what attackers are after. Companies therefore need to identify what their most sensitive data are and know exactly where they are located. Once the data have been categorized, they should be tagged and be subject to access restrictions. If organizations know exactly which of their data are particularly valuable, they can protect them specifically against attacks.

2 Creating copies and backups

The best defense against ransomware is performing regular and tested backups. Companies should employ the well-known 3-2-1 backup strategy: 3 copies of the data to be protected are created and stored on 2 different types of storage media. One copy of the data is kept offsite or offline. These clean backups are the key to recovery if the business falls victim to a ransomware attack. The sooner security managers, for example at the Cyber Defense Center, detect the infection, the less data are lost since the last usable backup. If the attack is stopped before the



criminals reach the backend systems, it is usually enough to reboot end devices without compromising business-critical data.

3 Practicing emergency drill

Conducting drills is important. Companies should a ransomware incident and practice the recovery processes. One of the primary points of focus here is to determine how much time the organization will need before it is fully operational again. These drills show managers what they need to do to improve their recovery processes. What is also often forgotten is that preparing for an emergency also makes it necessary to develop an internal and external communication strategy. Being able to communicate clearly in an emergency means being perceived as a reliable partner and supplier.

Prevention through security awareness and technologies

Prevention is the most effective strategy when it comes to minimizing the risk of a successful ransomware attack. Here are some best practice examples:

→ **Security training for employees against social engineering:** Educating and sensitizing employees is one of the most important measures for securing the company and its data. Email phishing is the most common method attackers are using to spread ransomware. In a phishing attack, cybercriminals pretend to be a trusted source and engage in fraudulent communication with their victim to trick them into, for example, opening an infected attachment, clicking on a malicious link or visiting an infected website. This means that it is important that employees know how to recognize phishing attempts. Companies need to create simple procedures for employees to report them to the company's security officers.

→ **Security solutions:** Email security filters, antivirus software and firewalls can block public and common strains of malware. Organizations should also deploy Endpoint Detection and Response (EDR) and Advanced Threat Protection (ATP) solutions to optimize ransomware detection and blocking.

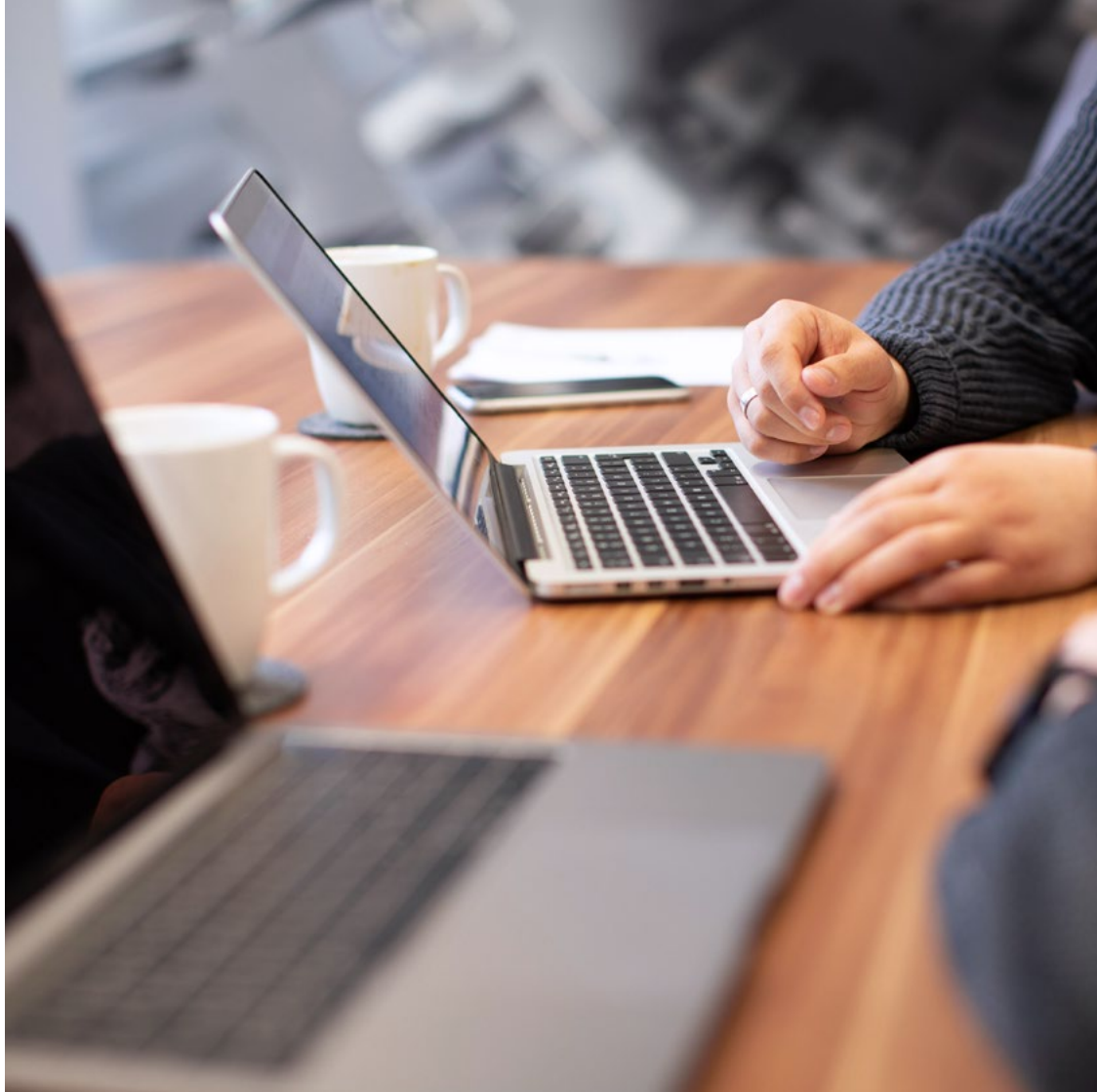
→ **Keep operating systems and applications up to date:** Unpatched operating systems and applications are easy prey for attackers and open doors for further attacks. This means that companies must ensure that their operating systems and software are always patched with the latest updates.

→ **Disable macros:** A number of ransomware strains are being sent as Microsoft Office attachments. When a user opens the attachment, they are prompted to enable macros to view the contents of the document. Once the user enables macros, the ransomware payload is downloaded and executed. This means that macros must be disabled by default, and employees must be informed that a request to enable macros is a warning sign.

→ **Manage access rights:** Users should only have as many access rights as they need to perform their tasks. Administrative rights should be limited as much as possible. It should also be ensured that administrative users must confirm all actions that require elevated privileges.

→ **Network segmentation:** This measure has a mitigating effect in the event of a ransomware infection, preventing the malware from spreading throughout the company's entire network.

→ **Penetration tests:** Penetration testing gives companies the opportunity to find vulnerabilities in the system and fix them before they can be exploited by attackers. Penetration testing should be performed at least once a year. A penetration test can also be useful when a major change is made to the company's network, such as changing the operating system and other changes in IT infrastructure.



24/7 Security guards: Cyber Defense Center (CDC)

When it comes to ensuring comprehensive prevention against cyberattacks, including ransomware and rapid response, organizations should consider running an inhouse Cyber Defense Center or implementing CDC as a Service, since both options can give a massive boost to their cyber resilience. Thousands of cyber threats come into being every minute. Technology can filter out many of the known threats, but only a Cyber Defense Center with around-the-clock service can help companies analyze the vast number of alerts, new threats and anomalies that the technical security infrastructure identifies.

A Cyber Defense Center – also known as a Security Operations Center (SOC) – combines IT security experts, processes and technologies. At the CDC, trained experts continuously examine Internet traffic, networks, desktops, servers, databases, applications and other IT systems for traces of a security incident. As a company's security command center, the CDC is thus responsible for continuously monitoring, analyzing and optimizing the security situation in order to quickly detect attacks and initiate appropriate countermeasures in the event of a security breach.

In-House Cyber Defense Center: For an in-house CDC, Radar Cyber Security offers companies a complete package of state-of-the-art, European-developed software, implementation and training. Experts support you during each and every phase – from planning and implementation to integration into your organization and continuous process improvement. Sensitive data remain with the CDC operator thanks to the on-premise solution.

CDC as a Service: Alternatively, the Radar Cyber Defense Center can take over the service for the client company. Highly trained experts at Vienna's Cyber Defense Center use cutting-edge technology to manage IT risk identification processes. Companies can find out their current IT security status at the push of a button, enabling them to take protective measures in good time with the support of the cybersecurity professionals from Radar Cyber Security.

First aid for a ransomware infection

No company is one hundred percent immune to a ransomware attack. Should an incident occur despite all security measures, the following steps are necessary, preferably initiated by a Cyber Defense Center or your security experts:

- **Isolate the infection:** To prevent the spread of the ransomware, all infected computers must be disconnected from each other, from shared storage, and from the network. The speed at which it is detected and isolated is critical to preventing ransomware from spreading throughout the network and encrypting critical data in a way that results in a costly recovery process.

- **Identify the malware strain:** Determining the malware strain with which the organization has been infected helps to understand how the ransomware spreads, what types of files it encrypts, and what removal and cleanup options are available. Often the ransomware identifies itself when it demands the ransom.

- **Report incident:** It is not only for compliance reasons that it is advisable to report the incident quickly to the authorities (such as in Germany or Austria the Federal Crime Investigation Office, the Federal Office for Security in Information Technology or the Data Protection Authority). These can assist with measures to defend against the attack and recover data.

- **Restore and update:** Affected systems must be wiped. Operating systems and application software must be reinstalled from scratch. After ensuring that the backups have not been infected, the data are restored and administrator passwords for all systems are changed.

- **Optimize protective measures:** Additionally it needs to be determined and analyzed how the infection actually happened along with measures being taken to make further attacks more difficult.

Defense in depth

Ransomware will continue to be one of the biggest threats for business continuity. One measure alone is not enough to protect your company, but with a layered security approach of ongoing employee training, robust business continuity processes, modern technologies and professional support from IT security experts, the risks and potential consequences can be mitigated which empowers companies to cope with today's challenges.

Would you like to receive more information on how a Cyber Defense Center can protect your organization from ransomware?

Get in touch with us!

RadarServices Smart IT-Security GmbH
Radar Cyber Security
Zieglergasse 6
1070 Vienna

E: sales@radarcs.com
P: +43 1 929 12 71-0

Subscribe to latest cyber security news:
newsletter-subscribe.radarcs.com

> "Let's face it and change our mindset: Cybersecurity has long since become part of the value chain."
>
> — Ali Carl Gülerman, CEO of Radar Cyber Security

RADAR CYBER SECURITY | Safeguard your digital journey.

RADAR Cyber Security is the only European provider of Managed Detection and Response solutions that offers its services based on its own proprietary technologies. More than 10 years of research have enabled a comprehensive technical platform solution for cyber security and IT risk detection. This is used on a daily basis to monitor the IT security of market leaders in various industries as well as in the public sector. Radar Cyber Security is a profound expert in machine learning for IT monitoring and continuously incorporates the latest findings into its services. Radar runs Europe's largest Cyber Defense Center in combination with its own Made in Europe detection technology at the head office in Vienna.

RadarSmart IT-Security GmbH
Radar Cyber Security
Zieglergasse 6
1070 Wien

T: +43 (1) 929 12 71-0
E: sales@radarcs.com
www.radarcs.com

Subscribe to first hand cyber security news: **newsletter-subscribe.radarcs.com**

PUBLIC

R_RANSOM_2021_EN_V1