USAID
OD AMERIČKOG NARODA

BOSNIA AND HERZEGOVINA ENERGY POLICY ACTIVITY

REPORT ON ANALYSIS OF ATTACK ON SARAJEVOGAS INFORMATION SYSTEM

JANUARY 2023
This publication was produced for review by the United States Agency for International Development.
Prepared by DT Global.

BOSNIA AND HERZEGOVINA ENERGY POLICY ACTIVITY

REPORT ON ANALYSIS OF ATTACK ON SARAJEVOGAS INFORMATION SYSTEM

JANUARY 2023

Contract No.:
72016819C00002

Prepared for:
USAID BiH Economic Development Office

Prepared by:
DT Global

CONTENTS

1 INTRODUCTION

KJKP "Sarajevogas" d.o.o. Sarajevo suffered an attack on its information system. As a result of the attack, information system services were rendered unavailable. IT staff managed to restore system functionality.

USAID's Energy Policy Activity prepared an analysis of the events based on available information. The purpose of the analysis is to share lessons learned from this case with other stakeholders in the energy sector.

On October 10, 2022, a meeting was held in the offices of Sarajevogas between representatives of Sarajevogas, USAID and USAID's Energy Policy Activity. Basic information about the attack was gathered at this meeting and a follow-up meeting to obtain more details was agreed. The second meeting was held on November 16, 2022 in the offices of Sarajevogas. At the meeting, Sarajevogas IT staff provided further technical details about the attack. This included insight into copies of files that were modified during the attack. An analysis of the event was produced based on the information gathered during these two meetings and from the copies of the relevant files, while also relying on expertise and available information about similar attacks.

The purpose of this document is to analyze the concrete attack, but also to point out potential gaps in information system security in the energy sector, with a special focus on the need for a coordinated and systemic approach to enhancing the security of information systems in the energy sector in BiH.

USAID's Energy Policy Activity had previously produced a report on the steps needed to achieve security of network and information systems in the BiH energy sector, as well as guidelines for transposing the NIS Directive in line with European Community and European Union cyber security regulations. Urgent implementation of these measures and guidelines is crucial for achieving quality and comprehensive protection of information systems at organizations active in the BiH energy sector.

2 SARAJEVOGAS IT STRUCTURE

The Cantonal Public Utilities Company "Sarajevogas" d.o.o. Sarajevo engages in natural gas distribution and trade through the distribution network. In addition, the company is engaged in the planning, construction and maintenance of natural gas distribution networks and connections. The company supplies cca 65,000 active natural gas customers divided into the following categories: households, small businesses, large businesses, KJKP "Toplane-Sarajevo" d.o.o. Sarajevo (district heating) and its Special Customer ("Sarajevo-gas" a.d. Istočno Sarajevo) for whom the company only transports gas. Sarajevogas maintains and manages a network of cca 1,128 km of low-pressure natural gas distribution pipelines with service connections.

The Sarajevogas IT infrastructure consists of network equipment and connections, servers, computers and additional equipment. Some of Sarajevogas's servers are not physically separate computers. Virtualization is used instead. Virtualization makes it possible to use a single physical computer (hardware) to run multiple (virtual) operating systems. Each of these operating systems functions as if it were installed on a separate hardware device. These operating systems are called

virtual machines. This way of installing operating systems and using hardware is very efficient and flexible. For this reason, most servers in contemporary environments are run as virtual machines. When it was modernizing its IT system, Sarajevogas opted to have only virtual servers. This made managing the servers easier and reduced costs. The fact that Sarajevogas servers are part of a virtualization platform is relevant for the description of the attack because the attack targeted this very platform. Therefore, the operation of this platform is presented below.

The software enabling virtualization is called a hypervisor. This is special software installed directly on the hardware to create a virtual layer between the hardware and the operating system. It is intended for creating and running virtual machines. There are various virtualization software developers. Sarajevogas uses software developed by VMware. This developer holds the majority of the virtualization market. The VMware hypervisor used by Sarajevogas is called ESXi. To facilitate the operation of larger numbers of virtual machines, VMware has additional software called vCenter Server. This software is used to manage servers. It enables automated setup of virtual machines and facilitates their operation. The software solution including the ESXi hypervisor and the vCenter Server virtual machine management software makes up the virtualization platform. The VMware virtualization platform is called vSphere.

To start up a virtual machine, or server with its operating systems, installed applications and data, the ESXi hypervisor uploads its configuration from files representing the virtual machine to be started up. These files contain all the operating system and virtual hardware settings, as well as all the data stored in permanent memory used to run the operating system. The data also includes the installed applications. Files for one virtual machine are commonly stored in a single folder. Each virtual machine has its own folder. Virtual machine files on the vSphere virtualization platform developed by VMware are stored in a separate file system called VMFS (*Virtual Machine File System*). VMFS is a file system adapted to storing files that represent virtual machines. A file system is a way to store files on the disk. VMFS differs from file systems used by most contemporary operating systems such as NTFS (Windows) and ext4 (Linux).

If files representing virtual machines are corrupted, the virtual machines cannot be started up. This is manifested as the server and all its services being unavailable.

3 DESCRIPTION OF THE ATTACK

On August 31, 2002, staff at Sarajevogas that use the information system noticed that it was not working. All of the services were unavailable. The running of all the business processes relying on the information system was disabled.[1]

IT staff tried to check on the status of the servers. They were unable to access the servers through the computer network. All of the servers they tried to connect to were unavailable. Instead of the expected dialogue box to enter access data for server administration, a message about the server being unavailable was displayed. They examined the virtualization platform directly. The reason for the servers being unavailable was found. All the files representing the virtual machines, i.e., the servers they had tried to access, had been modified. Due to these modifications, the ESXi hypervisor could not start up the virtual machines. Because the virtual machines could not be started up, the servers providing all the information system services could not be operated. In addition, backup copies of Sarajevogas data created by the Veem software had been deleted.

This method of hacking into and disabling the information system is not commonly seen in attacks. Usually, attacks target services available to external and internal users. At Sarajevogas, as at most organizations in the energy sector, these services are provided via virtual servers. A classic attack usually impacts only the data on the successfully hacked server. The attacker accesses data he should not be able to access, modifies data he should not be authorized to modify or makes the data unavailable to authorized users. This type of attack impacts one server or computer. The attack can then spread to other servers or computers, but this would require the attacker to circumvent the defenses of each new computer that is targeted.

The analyzed attack on Sarajevogas targeted the virtualization platform. This is a relatively new type of attack. It is highly damaging because disabling the virtualization platform also disables the operation of all (virtual) servers that are run from that platform. The attacker can thus halt the operation of the entire information infrastructure of the organization at once. This is exactly what happened.

3.1. RANSOMWARE

The attack was of the *ransomware* category. This is when an attacker encrypts the files on the attacked computer/server. When a file is encrypted, its original contents are modified and it becomes unreadable. To restore the original content, the file needs to be decrypted. After decryption, the contents of the file are restored to their original version and the file can be used normally. The attacker asks for a ransom payment to decrypt the files.

Encryption and decryption are mathematical transformations with an additional parameter called the key. A key is selected to encrypt the contents of files. The key is a sequence of bits. In order to decrypt the contents, you need the right key. What prevents decryption is not knowing the right key. This is one of the reasons why it is called a key, because it "locks/unlocks" contents.

The contents of encrypted files in a *ransomware* attack are rendered unavailable to the victim of the attack. Unavailability of contents means different things for different types of files. For files with data, such as text (e.g. Word) or tables (e.g. Excel), this means that the data from the files is rendered unreadable and cannot be displayed in their original form. For program or configuration files,

[1] The services provided by the Sarajevogas information system were not disclosed during our meeting. It is, therefore, impossible to list the specific business processes that were impacted. However, given the degree of digitalization, we can assume these include at minimum all administrative and financial processes.

unavailability of content means that the programs represented or configured by the original files cannot be run. In brief, encrypted files become unusable for their intended purpose. Attackers usually leave a note saying that they encrypted the files and provide instructions to the user about how to pay the ransom to have the files restored. After making the payment, the victim is supposed to receive the decryption key from the attacker. The name *ransomware* comes from the demand for a ransom to restore what was taken, in this case the data.

3.2. MODIFIED FILE EXTENSIONS

In the case of the attack on the Sarajevogas virtual infrastructure, in every folder with virtual machine files, all files with extensions (letters after the period in the filename) .vmx (VM configuration), .vmxf (additional VM configuration), .vmdk (virtual disk), .log (logs), .vmsd (VM saved data), .vswp (VM *swap* file), and .hlog (vCenter logs) were encrypted and given the additional extension of ._d0nut. Thus, for example, the original VM configuration file "Eracun.vmx" was encrypted and became "Eracun.vmx._d0nut". The extension name has no technical significance. It is an arbitrary sequence of characters selected by the malware developers to perform the *ransomware* attack. The extension names are usually different for each case of a *ransomware* attack. The attacks are also named after the extensions they use. As a result of these virtual machine files being encrypted, it was impossible to start up the virtual machines. This means that the servers, usually run as virtual machines, and the services they provide were rendered unavailable to users. In brief, the information system was down.

The only files that were not encrypted were those with the .nvram extension (BIOS or EFI VM configuration). Their encryption was not necessary to achieve the aim of the attacker, which was to disable the running of virtual machines.

3.3. MESSAGE FROM THE ATTACKER

In each of the folders, an identical READ.MD file appeared with instructions for how Sarajevogas could recover its data.

*/**
So what happened?

All files are encrypted with Integrated Encryption Scheme.
The file structure was not damaged. You have been assigned a unique identifier.
After infection, you have 96 hours to declare decryption.

After the expiration of 96 hours, decryption cost will be automatically increased.
Now you should send us message with your personal ID, which is at the bottom of the message.
We hope that you understand the importance of the work we have done.

Before paying you can send us 2 files for free decryption.
The total size of files must be less than 2Mb.
Files should not contain valuable information (databases, backups, large excel sheets, etc..).

Attention! If you want to RECOVER YOUR DATA without problems - NEVER!!! :
reboot, disconnect hard drives or take any action unless you know WHAT YOU ARE DOING!!!
Otherwise, we cannot be 100% sure that the decryptor will work correctly.

!!!THIS IS ESPECIALLY RELATED TO ESXI!!!

If you will try to use any third-party software for restoring your data or antivirus solutions:
this can lead to complete damage to all files and their irrecoverable loss.
Any changes in encrypted files may entail damage of the private key and the loss of all data.

Your personal id: A62A229AB534F137
Username and password are identical to above.

Since we are using SSL encryption as well as .onion, the certificate is not properly signed.
So in order to get into the chat, you need to confirm the insecure connection exception.
Or just use our embeded APP (Windows version only for now). Thank you for understanding.

You can download TOX here:
https://tox.chat/download.html

You can also write to the chat located in TOR network at:
https://qkbbaxiuqqcqb5nox4np4qjcniy2q6m7yeluvj7n5i5dn7pgpcwxwfid.onion

You can download TOR browser here:
https://www.torproject.org/download/

our TOX below:
D3404141459BC7206CC4AFEC16A3403F262C0937A732C12644E7CA97F061520IA519F7EAB2E2

We hope you carefully read this message and already know what to do.
**/*
D

The message has some particularities compared to what is common for messages of this type. The first is that there is no information about the amount of money that needs to be paid, or a Bitcoin, or any other address, where the payment is to be made. The victim is asked to contact the attacker through the TOX application for secure messaging (*chat*). This is an application akin to Viber or WhatsApp, but the application developer does not have a central server that can be monitored. Instead, the application uses a *peer-to-peer* connection system. The aim is to reduce the possibility of surveillance and control over messaging participants and content. The attacker's TOX identifier is also given. This information can be used to help find other victims of the same attacker and connect multiple attacks. The message also gives the victim's personal ID. This ID can also be used to search for similar attacks. The message specifically refers to the ESXi hypervisor. This can mean that it was designed specifically to attack the VMware virtualization platform.

In addition to this expected result of the *ransomware* attack on the virtualization infrastructure, the attackers made it additionally difficult to remedy the impact of the attack by deleting the backups of Sarajevogas data made using Veem software. These included backup copies of all data stored by Sarajevogas. They were kept precisely for the purpose of recovery after an event where the original data is lost. With this, the attackers wanted to increase their chances of receiving payment. The practice of attackers deleting backups during, or usually immediately before an attack, is not unheard of, but it is relatively new. Such practices were first observed in 2020. In order to be able to delete the backups, the attackers had to have had access rights of users responsible for managing the backups. This means that the attackers accessed the system as system administrators, i.e., they somehow obtained the access data or used a weakness in some software that was run by the system administrator.

4 RECOVERY FROM THE ATTACK

The main negative effect of the attack was that the Sarajevogas information system services were made unavailable. This means that all business processes for which the information system was needed were stopped. The natural gas supply system is not managed through the information system, so this functionality was not at risk. Nevertheless, stopping certain business processes results in material costs. These costs can be estimated to a degree. In addition to material losses, inestimable damage to the company's reputation is also incurred. For this reason, the first objective was to enable the running of the information system and continue normal operations at the company.

We should also look to the future when managing the natural gas supply system will be done through the information system. In this near future, an attack such as this one could bring natural gas supply to a complete halt. That could have catastrophic repercussions, especially in the winter period, when it could put people's lives at risk.

Modified and deleted files are restored from their backup copies. In this case, quickly restoring virtual machine files from easily accessible backup copies using the Veem software was not possible. These files, partly due to how easy they were to access, had been deleted during the attack. In line with good practices, Sarajevogas had additional backups that were not directly available for restoring, but this made them also more difficult to access by attackers. These copies, as is common for second backups, were kept on magnetic tapes.

Magnetic tape for keeping data is similar to magnetic tape used in audio and video cassettes. It can be used to store large amounts of data, but the data have to be accessed in the right order. This means that the tape has to be rewound to the position where a piece of data is located. By comparison, data on hard disks is accessed directly, without the need for rewinding. Because of the writing and

reading of data from tapes, the process of storage and recovery takes a lot more time compared to hard disks. Special devices are used to read and write magnetic tapes. Tapes are inserted into the device for something to be written on them or read off them. When not used, the tapes are stored outside the device. Even though the tapes have high capacity, the amount of data that needs to be backed up is so large that multiple tapes are needed. This makes tapes relatively impractical, but on the other hand, quite secure for storing backup copies. In order to delete or modify the backups, an attacker would have to have physical access to the tapes. Of course, the tapes need to be physically protected from damage and theft.

Since the attack on Sarajevogas only impacted its information system, the data stored on the tapes was not at risk. This enabled the Sarajevogas IT staff to successfully restore the correct copies of all virtual machine files. They also reinstalled the VMware virtualization software that is being used. This step was performed in order to eliminate the possibility of any software from the attacker remaining on the virtualization platform used by Sarajevogas. The reinstalled virtualization software and correct copies of virtual machines made it possible to start up the virtual machines. This is how all the servers of the Sarajevogas information system and all the services they provide were restarted. All the information system services were available once again. All business processes depending on them could be performed.

It should be noted that some data is always lost when restoring files from backup copies. Some of the lost data is data created from the moment when backup copies were made to the moment of the event that requires restoring from backups. The amount of data that will be lost depends on how often backups are made and on the rate of generation of new data. In the case of Sarajevogas, this information was not available.

It should be noted that in this case, all procedural safeguards in line with professional standards were in place, and they require having multiple backup copies. It is also important that the backup copies were not faulty and could be used to restore data, which is not always the case.

5 ANALYSIS OF THE ATTACK

5.1. ATTACKER – "DONUT LEAKS"

Based on the gathered data, a search for similar attacks was conducted. The ".d0nut" extension added to encrypted files gave this *ransomware* its name as "d0nut *ransomware*." The first documented attacks with this *ransomware* date from the second half of 2022. In addition to the extension, the attacks also had an identical or very similar message from the attacker. The same TOX *chat* identifier D3404141459BC7206CC4AFEC16A3403F262C0937A732C12644E7CA97F0615201A519F7EAB2E2 and the same TOR *chat* address https://qkbbaxiuqqcqb5nox4np4qjcniy2q6m7yeluvj7n5i5dn7pgpcwxwfid.onion appeared in all the messages. These identifiers are connected to the attack group known as "donut leaks". The provenance of this group is unknown. It is responsible for at least 10 attacks. Three of the 10 companies came out in public about being attacked. They are:

1. Sheppard Robson, an architecture firm in the UK on July 24, 2022
2. Sando, a multinational construction company in July 2022
3. DESFA, a Greek natural gas company on August 20, 2022.

The other victims have not come out publicly, so their names are unknown. The minimal number of victims was determined based on the website available through the anonymous TOR web browser. The group "donut leaks" published some of the data taken from the attacked companies on this

website. There were 10 companies whose data was made available. The purpose of publishing the data was to humiliate the victims and force them to pay the ransom. It is also related to the name of the group "leaks," because they "leak" company data to the public. It is interesting that the attackers' group Ragnar Locker claimed responsibility for the attack on DESFA, and Hive Ransomware claimed responsibility for the attack on Sando. It is believed that Donut Leaks was originally behind the attack, but some of the data from some of the attacks reached other groups, possibly through members who switched groups. The same TOX *chat* identifier also appeared in attacks with HelloXD *ransomware* from November 2021, which were linked to the group x4k. A detailed description of the *ransomware* was provided by Unit 42 of the PaloAlto security company.[2] The best description of how Donut Leaks operates was published by BleepingComputer in two articles, dated August 23, 2022[3] and November 22, 2022.[4]

5.2. SPECIFIC CHARACTERISTICS OF THE ATTACK ON SARAJEVOGAS

What is specific about the Sarajevogas attack is that, in contrast to attacks on other companies performed using the same *ransomware* (d0nut) by the same group (Donut Leaks), in this case the attack targeted a virtualization platform. In all other cases, the ransomware attack was performed directly against computers/servers, and not a virtualization platform. As pointed out before, an attack on a virtualization platform has more far-reaching consequences that an attack on an individual server or computer. When a single server is attacked, only that server becomes unavailable. An attack on a virtualization platform makes all servers unavailable.

The reason for attacking the virtualization platform may be that in the case of Sarajevogas, the attackers managed to gain access to the virtualization platform, and then decided to perform an attack on it. Furthermore, Sarajevogas was not notified that the stolen data would potentially be published in order to exert additional pressure on the company to pay the ransom. Still, the same contact information is an indication that the attack was performed by the same group.

It was impossible to determine how the attackers managed to run their file encryption malware. It was also impossible to determine how they managed to access the Veem backup copies of data and delete them. This would have required logging into the system as administrators. It was not possible to determine how the attackers managed to get hold of access data in order to log in as the system administrator. No traces of infection with malware were found on the examined personal computers at Sarajevogas. When the data was being restored from backup copies and the VMware virtualization software was being reinstalled, and all the potentially infected computers at Sarajevogas were being recovered, traces were copied that could perhaps indicate the source and path of the attack. This situation commonly occurs during attacks. The organization wishes to restore functionality as soon as possible. This means undertaking steps to remove the attack. On the other hand, organizations, and especially law enforcement agencies, want to gather traces that will help them determine how the attack occurred and where it came from. Both aspects need to be taken into account and an appropriate plan needs to be devised when developing incident response plans.

One possible path of the attack is a remote connection to the Sarajevogas network used by the company working on the Sarajevogas SCADA system. According to information received from Sarajevogas, this connection gave the partner company unlimited remote access to part of the

[2] https://unit42.paloaltonetworks.com/helloxd-ransomware/

[3] https://www.bleepingcomputer.com/news/security/new-donut-leaks-extortion-gang-linked-to-recent-ransomware-attacks/

[4] https://www.bleepingcomputer.com/news/security/donut-extortion-group-also-targets-victims-with-ransomware/

Sarajevogas system they were working on. Another possible path the attackers may have used to access the virtualization platform were the connections from some of the IT staff computers on the platform. These connections enabled IT staff responsible for maintenance of the virtualization platform to perform these tasks from their own computers, without having to physically access the server from which the platform was run. This is common practice when it comes to managing virtualization infrastructure. The attackers could have infected and taken control of the computer of an IT staff member. The connection of that computer with the virtualization platform would then be exploited for the attacker to connect and encrypt the files. However, no traces of malware were found on these computers either. This can mean that this was not the first time they were attacked or that the attackers removed their malware once the attack was completed.

The paths of attacks usually involve tricking users or exploiting an insecure connection to the internal network. Users are tricked into entering their access information on a fake site or running software from an e-mail attachment or an ostensibly useful site. The attacker uses the stolen access information to gain access to the system of the user from whom the information was stolen. In this way, the attacker gains access to resources inside the organization that are the target of the attack, in this case the encryption or deletion of data.

When the user is tricked into running software planted by the attacker, the software obtains the user access rights of the user who runs it. Having obtained these rights, the software can then encrypt and delete data or give the attacker remote access to the system, as with stolen access information. If the organization's information system has an active connection giving access to connected users for the purpose of system maintenance or upgrade, this kind of access can also be abused. It is possible for system access information to be hacked or stolen. Another option is when attackers breach the system of external associates and thereby exploit the connection the associates have with the organization that is the ultimate target of the attack.

6 CONCLUSIONS AND RECOMMENDATIONS

6.1. THE ENERGY SECTOR IN BIH CAN BE A TARGET

The most important takeaway is that attacks such as this one also happen here in Bosnia and Herzegovina. Energy sector companies can also be targeted by attacks. An increase in the number of these attacks should be expected. With the arrival of winter and the potentially very limited energy supplies available in Europe, energy companies are liable to become increasingly susceptible to extortion. Readiness is key. This means reducing the risk of companies being victimized by a successful attack and reducing the potential impact of such attacks.

It is very important for all companies and organizations active in the BiH energy sector to put this issue on their agendas, perform internal reviews of vulnerabilities and actively work to protect their systems and information.

6.2. ADOPTION OF LEGAL FRAMEWORK AND EDUCATION

Adopting the required legal framework to stipulate all aspects of cyber security in BiH is needed as a precondition for a systemic approach to solving these issues.

In addition to everything mentioned above, it is necessary to continuously raise public awareness about this problem and its prevalence, with continuous education on the scope of the problems that can be caused by cyber attacks.

6.3. IMPROVE INFORMATION EXCHANGE IN THE ENERGY SECTOR

The second lesson learned is that the attacked companies find themselves not knowing who to reach out to. Their only contacts are law enforcement agencies. These deal with the criminal responsibility of the attackers. For technical assistance and support, companies have to contact private firms. This is usually a necessary step, but it can be preceded by other useful steps. Well-established information exchange between companies in the energy sector would enable them to learn from each other's experiences. This can help companies be better prepared for attacks that have already happened somewhere else. It can facilitate stopping the attack and removing the damage. Also, companies from the sector can share their experiences with hiring private firms to recover from attacks. One common form this kind of cooperation takes is the energy sector CSIRT. Steps should be taken to establish it. To begin with, this can be a less formal group of information security staff from energy companies. With time, it can become a real formal CSIRT.

6.4. BACKUPS ARE NECESSARY

With attacks that target availability of data, the most important form of protection is having backup copies of the data. Dedicated software should be used to make these copies. Irrespective of the software used, the 3-2-1 rule should be observed.[5] This means that there should be three copies of all important files. One primary and two backups. The copies should be stored on two different kinds of media. One copy should be stored in a different physical location from the original data. Backup copies do not only protect from *ransomware* attacks. They also enable data recovery in all other cases when data are deleted or unavailable due to an attack, legitimate user error or natural disaster.

6.5. PROTECT THE VIRTUALIZATION PLATFORM

Attacks on virtualization infrastructure will become increasingly frequent. They are very effective for the attacker, because a single successful attack puts at risk the entire IT infrastructure of the organization. Energy sector companies tend to be large, which means they have large IT infrastructures. Today, such infrastructures are mostly virtualized. This also means that BiH energy sector companies can also be targeted by these attacks. These companies need to review and reinforce the protection of their virtual infrastructure. Many defenses focus on defending individual services and/or individual servers. These defenses should remain in place. They should be complemented by infrastructure defenses. These should include both technical and physical measures that restrict access to infrastructure. This is called defense-in-depth or layered security and is the recommended approach to building defenses.

6.6. USE MULTI-FACTOR AUTHENTICATION

Reducing the risk of successful attacks can also be achieved by severing the paths of attack. According to statistics,[6][7] the most common paths of attack are theft of access data and exploitation of security gaps in publicly available services. These attacks are often performed against partners of the organization that is the ultimate target. Partners with access to the organization's internal

[5] Paul Ruggiero and Matthew A. Heckathorn, "Data Backup Options", CISA/US-CERT, 2013.
[6] John Pescatore and Terry Hicks, "SANS 2022 Top New Attacks and Threat Report", SANS, 2022.
[7] "Microsoft Digital Defense Report 2022", Microsoft, 2022.

network are attacked. Statistics should be used to set security priorities. Theft of access data is done by tricking or hacking users. Users can be protected from fraud through training. Access data can be protected from hacking through reasonable policies on the complexity of such data. In both cases, using multi-factor authentication methods to log into the system are recommended for good security. Today, this most often means that in addition to a password, the user will also have to input a number generated by software on the user's phone. This method of logging in should be mandatory for critical systems such as virtualization platforms.

6.7. REGULARLY UPDATE OPERATING SYSTEMS AND SOFTWARE

Security gaps exploited by attackers are removed by regularly updating software. In the case of software that cannot be updated, which happens in the energy sector due to long lifetimes of dedicated hardware and software, then other security measures need to be undertaken to prevent the exploitation of non-updated software. All partners that are given remote access to the system must prove that they have in place security measures that are at least identical to those of the organization to which they are being granted access.

Of course, additional security measures can also be applied. In the interest of applicability and brevity, priority measures are given above.

United States Agency for International Development

www.usaid.gov