Network and System Administration CA4

In-Depth Activity

Universitat Oberta de Catalunya

Nicolas D’Alessandro Calderon

Bachelor's degree in Techniques for Software Application Development

Course instructor

Jaume Jofre Bravo

Date of submission

May 30, 2025

Table of Contents

Table of Figures

01
INTRODUCCION

Ransomware has become one of the more dangerous and persistent cybernetic threats in the current context of the companies. What began in 1989 with the Trojan AIDS case, a rudimentary program that was distributed on floppy disks, evolved into very sophisticated techniques such as phishing campaigns or the Remote Desktop Protocol (RDP).

The most common type is the **cryptographic ransomware**. This consists in blocking the access to files using cryptographic techniques, so the attackers will then send messages to the victims (a particular person or a company), called ransom notes, demanding payment to recover the information. Famous examples of this type are CryptoLocker, WannaCry o Ryuk.

Another common technique is **locker ransomware**, which “locks” the access to the entire device rather than encrypting files. The modus-operandi includes displaying a screen that block the access (many times simulates being an original message coming from an official authority such as the police) so even the files are not affected, it completely paralyzes the device.

In recent years, a more aggressive version became very popular called **double extortion**. This is a technique used by attackers that combines *crypto ransomware* with an additional threat:

1. *First extortion*: They encrypt the victim's files and demand a ransom to recover them.
2. *Second extortion*: They threaten to publish the stolen data (exfiltrated before encryption) if the ransom is not paid.

The consequences on reputation can be equally devastating. Losing the trust of customers, partners, and shareholders can take years to reverse, and in some cases, organizations must also face legal and regulatory sanctions, especially if personal or confidential data is compromised.

In this context, we can say that ransomware is not just a technical issue, it is also a strategic one. It is very important for the current companies to understand how it works, how it evolves (being updated on latest techniques), and the impact that this may have, if they want to protect its operations and digital integrity.

Finally, we may say that understanding the problem is only the first step. Companies must focus on preventing these attacks, detecting them early, and taking steps to minimize their effects when they occur.

02
PREVENTION STRATEGIES

Organizational Policies and Staff Awareness

After reading much about ransomware, I believe that one thing is very clear: stopping an attack before it happens is much easier and cheaper than fixing the damage after. All the articles, and bibliography mentioned that Prevention is the most important part of a good cybersecurity plan. There is no perfect way to stay 100% safe, but there are many best practices that if we follow them well, we can lower the risk of an attack.

One key action is to divide the network into smaller parts and give users only the access they really need. This helps stop attackers from moving around the system if they get inside. At the same time, giving fewer permissions means that if one user account is attacked, the damage will be smaller.

Keeping systems updated is also mentioned as very important. Many ransomware attacks use old problems in software that have not been fixed, so by installing updates and checking for weak points often, we may close those doors before attackers can use them.

The security is not just the technology used. People are also a very important part. Many ransomware attacks start because of human mistakes and that's why companies need clear rules and training for workers regarding these topics, such as phishing email campaigns, fake messages, etc. Staff should learn how attacks happen and how to stay safe. These trainings should not be done just once. It should happen often and change when new threats appear.

A good idea is to send fake phishing emails to the employees as a test. These emails are safe but look real. When the person learns to recognize and report them, they are better prepared for real attacks. In my personal experience, I have been working in different companies that adopted this methodology, and I can tell that learning from the experience of reporting and understanding fake emails is much better than reading trainings or courses.

It’s also important to have a culture where people feel safe to report problems. Workers should feel like they are helping the team, not that they will get in trouble. The leadership should support this and make security a company value. When that happens, everyone helps to keep the organization safe.

It is also a good idea to follow known cybersecurity guides like the NIST Framework, ISO/IEC 27001, or the CIS Controls. These frameworks give the knowledge of the steps to protect the company. Using them shows good practice, and it also builds trust with customers, partners, and regulators.

03
PROTECTION SYSTEMS

To protect against ransomware, companies need special systems that can see attacks early to stop them and keep them from spreading. These systems are different from employees training or company rules. They work directly on the computers, networks, and data, and need experts to set them up.

A big part of protection is keeping the endpoints (like computers, laptops, and servers) safe. These are common targets in attacks. Old antivirus tools are not enough now. New tools like **EDR** - Endpoint Detection and Response and **XDR** - Extended Detection and Response are better. They don't just find known viruses, they also watch for strange behavior, like many files being locked fast, attackers moving inside the network, or backup files being deleted.

But it's not enough to protect just the computers. We also need to see what's happening on the network. Tools called NDR - Network Detection and Response look at network traffic. They try to find unusual actions, like ransomware spreading or data being stolen.

These tools work well when used with **SIEM** systems. SIEM means "*Security Information and Event Management*." It collects events and alerts from different parts of the system and finds connections between them. This helps us notice bigger attacks.

We also have **SOAR** platforms. SOAR means "Security Orchestration, Automation and Response." These tools help us react quickly. For example, if something dangerous is found, SOAR can automatically isolate a computer or block a user account.

Another important part of protection is having safe backups. New backup systems can make files unchangeable for some time, and can store copies offline, so that the ransomware cannot reach them. Some tools also send alerts if the backup size or activity looks strange.

The best defence comes when all these systems work together. For example, if the EDR sees something bad, it sends an alert to the SIEM. The SIEM can then tell the SOAR to take action fast like cutting off the infected device. This fast teamwork can stop big problems before they spread.

It is important to remember: these tools cannot stop every attack. But they can help us see danger early and act fast to reduce the damage.

04
RESPONSE AND RECOVERY IN THE EVENT OF AN INCIDENT

Incident Response Steps

Even with the best protection, no system is 100% safe. We already mention that, but it is probably the most important takeaway of these activity. When a company is attacked with ransomware, the first question is sometimes not technical but if they should or not pay the ransom.

From an ethical point of view, paying is not good. It helps the criminals because if companies pay, attackers continue because they see it works. Also, there is no promise that the attackers will give back the data or not attack again.

Legally, this is also a difficult topic. In many countries, paying is not illegal. But if the stolen data is very private, like health data or personal info, there can be legal problems. If the company pays and does not tell the authorities, it can be seen as a mistake or even as hiding the truth, ending in legal consequences.

Most security groups like CISA, the FBI, or ENISA say **do not pay**. That's why it is important to have a clear plan to respond to ransomware. This helps control the damage, return to normal, and learn from the attack.

Good practices from groups like NIST and ISO say the response must follow these steps:

1. **Detection**: This is the first step where we need to know something is wrong. Maybe there is a ransom note, or maybe the system gives alerts of strange activity.
2. **Analysis**: Next, the security team checks what was attacked, how the attackers got in, and if they took data. It is important to write everything down. This helps in later steps, and for the reports to authorities or insurance.
3. **Containment:** Now we stop the attack. We isolate the infected systems by unplugging devices, turning off the Wi-Fi, or blocking bad accounts and IPs. **Speed is very important here**.

4. **Eradication**: This step removes all the traces of the ransomware. It also fixes the weak points that the attacker used by reinstalling systems, updating software, changing passwords, deleting bad accounts, etc.
5. **Recovery**: Now we bring back the systems and data using good backups. We must test that everything is safe and working well. This step also includes restarting the business activities, talking to users, and watching the systems for any new problems.
6. **After incident review:** After recovery, we learn from what happened. We improve our rules and systems. It is also a good time to check the backup policies, update the response plan, and train the employees again.

Communication is also very important in every step. Inside the company, everyone must know what to do and what not to do (for example: do not turn off infected computers). Outside the company, we may need to tell the authorities or the public, depending on the size of the attack. Clear and fast communication is very important during this whole process.

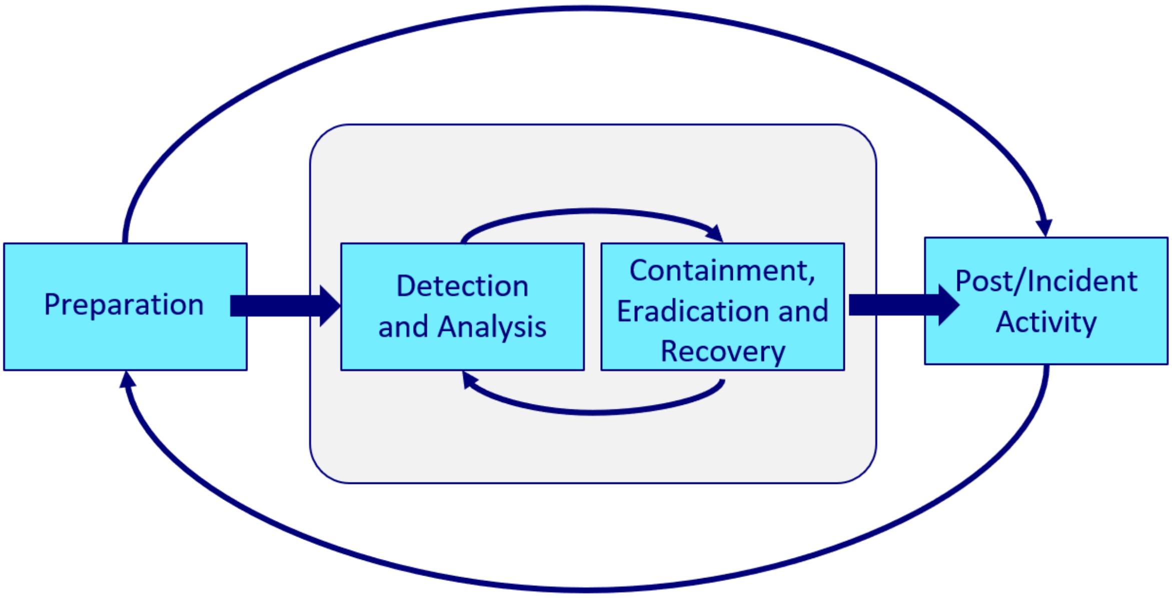

Figure 1- Response to Incidents

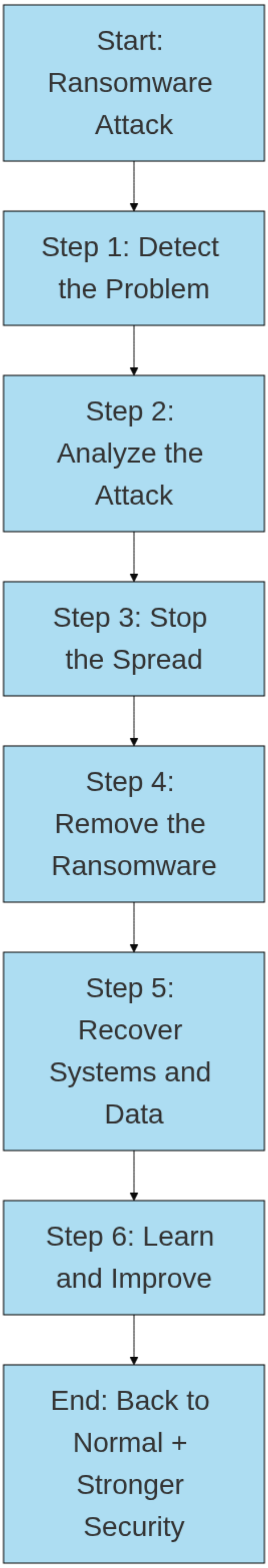
Start: Ransomware Attack
Step 1: Detect the Problem
Step 2: Analyze the Attack
Step 3: Stop the Spread
Step 4: Remove the Ransomware
Step 5: Recover Systems and Data
Step 6: Learn and Improve
End: Back to Normal + Stronger Security

Figure 2 - Incident Response Steps

05
SOLUTIONS CURRENTLY AVAILABLE ON THE MARKET

Today, there are many tools in the technology market that helps with different parts of a cyber-attack. These tools are useful, but we have to be very careful with the decision of which one to choose, because we need to know what they can do, and also what they cannot do, especially in big companies.

To protect devices like servers, PCs, and phones, there are very used tools like **Microsoft Defender for Endpoint**, **CrowdStrike Falcon**, **SentinelOne**, and **Sophos Intercept X**. These tools use a combination of behavior detection, machine learning, and automatic actions. They are strong options to stop many threats before they happen, and some can even undo changes using local backups. But these tools only work well if we set them up correctly and keep them updated. Also, some tools like **ED Silencer** and **Sandblast** can stop these protections before starting a ransomware attack. So, this is a clear example that there’s no perfect tool.

For networks, tools like **Darktrace** and **ExtraHop Reveal(x)** help find strange activity. This is useful for detecting ransomware that is spreading in the system or data that is being stolen. These tools are good because they can see things that other tools on the devices cannot see, especially on devices like IoT or old systems.

There are also other tools for the **SIEM** category already explained, like **Splunk**, **QRadar**, and **Microsoft Sentinel**. They help to collect and connect logs from many places to find big attacks. SOAR platforms, like Cortex XSOAR and **TheHive**, can help act quickly when there is a problem.

If there is an attack, it is important to have good backups. Tools like **Veeam**, **Commvault**, and **Acronis** help make safe backups, send alerts for problems, and recover fast. But these only help if we test them and keep the backup storage safe. Sometimes, backups are also encrypted because they were not protected well.

There are also open-source tools like **Wazuh, Zeek, and Bacula**. These are cheaper and more flexible, but they are harder to use and require a strong technical team. They do not have professional support, which can be a problem during an emergency.

Finally, MDR services (Managed Detection and Response) are now more popular. They help companies that do not have their own security team. MDR gives 24/7 protection and fast action. But it also has problems since clients cannot always see what is happening, and not all services are the same. The price can also be too high for some companies.

06
CONCLUSIONS AND PERSONAL ASSESSMENTS

After analyzing Ransomware characteristics and its different aspects, I may say that we are not facing only a technology threat but a real challenge in organizational management, which requires us to combine technical knowledge, solid process and organization, but above all, collective awareness.

One of the most repeated ideas is that there is no single solution. And I think that's a key lesson. Security against ransomware doesn't depend only on installing "the best tool," but on having a coherent and realistic strategy. I've noticed that many companies fall into the trap of investing large sums of money in sophisticated software, but neglect the basics, such as making verified backups, keeping up-to-date updates, and providing ongoing training for their staff. I was also struck by the number of layers a good defence can have. From email filtering to network traffic analysis, including endpoint detection and automated response. It's a living system that must be well-oiled, and that requires time, resources, and, above all, commitment from company management.

As a personal experience, this work made me more aware of the importance of understanding how these attacks work. I often see them as something that only happens to large corporations, but the reality is that more and more small and medium-sized companies are being targeted precisely because they have less preparation or resources. And the damage they can suffer is also very profound.

If I had to give one general recommendation on the subject, it would be to be prepared before it happens. Be clear about what you would do if tomorrow, for example, all of your organization's files were encrypted, because the time to define that plan isn't during the crisis, but long before. And in that sense, continuous learning, scenario simulation, and teamwork make all the difference. I can now say that cybersecurity is a much more human and strategic field than it seemed at first glance. And that, as in many other situations, prevention and anticipation end up being much more valuable than hasty reactions.

07 BIBLIOGRAPHY

IBM. (s.f.). What is ransomware? IBM. https://www.ibm.com/think/topics/ransomware

IBM. (s.f.). Ransomware-as-a-Service (RaaS). IBM. https://www.ibm.com/think/topics/ransomware-as-a-service

Sophos. (s.f.). The State of Ransomware. https://www.sophos.com/en-us/content/state-of-ransomware

UK Government. (2023). The experiences and impacts of ransomware attacks on individuals and organisations. https://www.gov.uk/government/publications/the-experiences-and-impact-of-ransomware-attacks-on-victims/the-experiences-and-impacts-of-ransomware-attacks-on-individuals-and-organisations#executive-summary

Zscaler. (s.f.). What is network segmentation. https://www.zscaler.com/es/resources/security-terms-glossary/what-is-network-segmentation

Hackmetrix. (2021, abril 13). Cómo prevenir y protegerse contra el ransomware. https://blog.hackmetrix.com/como-prevenir-y-protegerse-contra-el-ransomware/

National Institute of Standards and Technology (NIST). (s.f.). Cybersecurity framework. https://www.nist.gov/cyberframework

Smart Industry. (2023, octubre 10). Why ransomware attackers target backups. https://www.smartindustry.com/benefits-of-transformation/cybersecurity/article/55263751/why-ranomware-attackers-target-backupsand-how-to-ensure-your-data-is-protected

Cybersecurity & Infrastructure Security Agency (CISA). (2020). Ransomware guide. https://www.cisa.gov/stopransomware/ransomware-guide

Fortinet. (s.f.). Incident response glossary. https://www.fortinet.com/lat/resources/cyberglossary/incident-response

Veeam. (2023, marzo 16). Ransomware response plan. https://www.veeam.com/blog/es/ransomware-response-plan.html

Halcyon. (2023, noviembre 14). EDR killers used to bypass security in ransomware operations. https://www.halcyon.ai/blog/edr-killers-increasingly-used-to-bypass-security-in-ransomware-operations

Balarabe, T. (2023, julio 24). What is ransomware? Understanding and defending attacks. Medium. https://medium.com/@tahirbalarabe2/what-is-ransomware-understanding-and-defending-attacks-75d9f55d6470

Soto, M. (2023, agosto 3). El ransomware sigue siendo el rey del baile. Medium. https://marvin-soto.medium.com/el-ransomware-sigue-siendo-el-rey-del-baile-cfae27f11845

Guayoyo. (2022, marzo 14). Ransomware: Qué es y cómo se transmite. Medium. https://medium.com/guayoyo/ransomware-qu%C3%A9-es-y-c%C3%B3mo-se-transmite-c187eba516b4

Cyber Magazine. (2023, julio 12). Top 10 ransomware defence platforms. https://cybermagazine.com/hacking-malware/top-10-ransomware-defence-platforms

Palo Alto Networks. (s.f.). Ransomware response and recovery. https://www.paloaltonetworks.com/cyberpedia/ransomware-response-and-recovery