

Ransomware Report 2025

Learning from each other's data breaches

AP

July 2026

1. Year Review 2025: ransomware attacks continue, risks are increasing

Summary

- Ransomware attacks remain common. Every successful attack is one too many. The risks to people of scams and identity fraud are increasing. This is because data is increasingly stolen in ransomware attacks. Criminals can combine stolen data from various data breaches.
- The Autoriteit Persoonsgegevens (AP), the Dutch data protection authority, is calling on organisations to learn from one another. Ransomware and other cyber attacks occur frequently and across all sectors. Organisations must implement crucial security measures aimed at preventing data breaches. And prepare in the event things do go wrong.

Introduction

Ransomware attacks are one of the most serious types of cyber attacks. A ransomware attack nearly always involves personal data of a large number of people at once. Because the AP must always be notified of data breaches of this kind, the AP has obtained a broad overview of the ransomware situation in the Netherlands.

The AP intends to share its insights by means of a special ransomware report, allowing organisations in the Netherlands to apply these insights.

The AP also calls on organisations to learn from each other by sharing experiences and tips about ransomware.

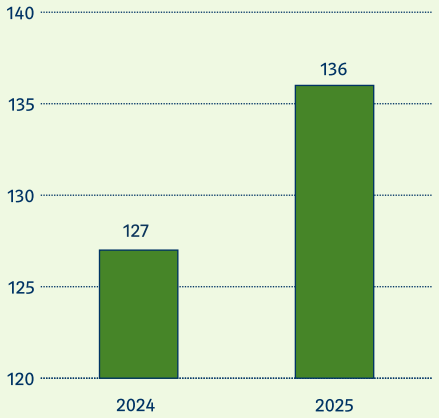
The AP also gathers experiences and lessons learnt, and shares these: the AP spoke to organisations that were victims of a ransomware attack in 2025.

You can read their tips and experiences on page 6.

Figures: ransomware attacks are as frequent as ever

In 2025, the AP recorded 136 ransomware attacks. In 2024, this number stood at 127. Ransomware attacks remain as common as ever.

FIGURE 1 | Ransomware attacks in 2024 and 2025



The number of data breach notifications that were caused by ransomware attacks is higher than the total number of attacks. This is because a single attack can sometimes affect multiple organisations, for example when a supplier to several organisations has been attacked. In that case, each affected organisation reports its own data breach. In 2025, the 136 ransomware attacks resulted in at least 283 data breach notifications.

What is ransomware?

Ransomware is a portmanteau of the words ransom and software. In these attacks, cyber criminals can encrypt and steal data and threaten to publish it. Increasingly, cyber criminals steal data without encrypting it. Since 2025, the AP has also classified these attacks as ransomware attacks.

Ransomware has major consequences

Ransomware attacks directly impact digital security. Attackers may not only steal personal data but can also shut down critical digital processes and services. Therefore, few data breaches have such a major impact as ransomware.

The attack on the laboratory behind the Dutch Centre for Population Screening in 2025 showed how hundreds of thousands of patients were affected at once. Because these types of attacks continue to occur annually, people report that they have been victims of a major data breach on multiple occasions. The damage to the victims is accumulating.

Substantial financial damage

In addition, a cyber attack costs the affected organisations an enormous amount of money. Research by the AP shows that the damage to organisations runs into the hundreds of thousands of euros. Money that could also have been spent on preventing attacks.

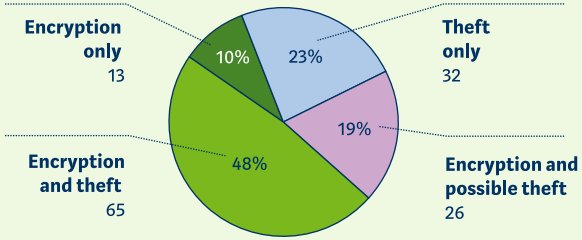
Precisely for this reason, the AP not only investigates the data breach itself in the case of ransomware, but also looks at how organisations are prepared for cyber incidents and handle the consequences for victims.



Increasing data theft

Ransomware comes in various forms. Attackers often encrypt and steal data. This was the case in 65 ransomware attacks in 2025. Sometimes, attackers only encrypt the data (13 times). In 26 ransomware attacks, the AP was able to determine from the report that data had been encrypted, but it was unclear whether the attackers had also stolen data. The attackers frequently only stole data, without encrypting it (32 times). The AP observed this only 15 times in 2024. Data theft is a worrying development, as stolen data enables further misuse, with serious consequences for the victims.

FIGURE 2 | Types of ransomware attacks in 2025



Data breaches caused by ransomware attacks affect various sectors, victims and personal data

In 2025, most notifications of data breaches caused by ransomware attacks came from the health and welfare, trade and automotive, and information and communication sectors.

Data breaches resulting from a ransomware attack affect different types of victims and different types of personal data are breached. This often involved the personal data of employees of the hacked organisation. It regularly involved the personal data of customers and sometimes the personal data of vulnerable groups, such as patients or underage victims.

In data breaches caused by a ransomware attack, mainly contact details are compromised. Criminals use this data for scam messages. In approximately one-third of these data breaches, citizen service numbers (BSNs) and copies of passports were also leaked. Criminals can use this data for identity fraud. Stolen datasets can also be combined. In that case, people become victims of the accumulation of these data breaches over the years.

FIGURE 3 | Sectors with the highest number of reported data breaches caused by ransomware in 2025

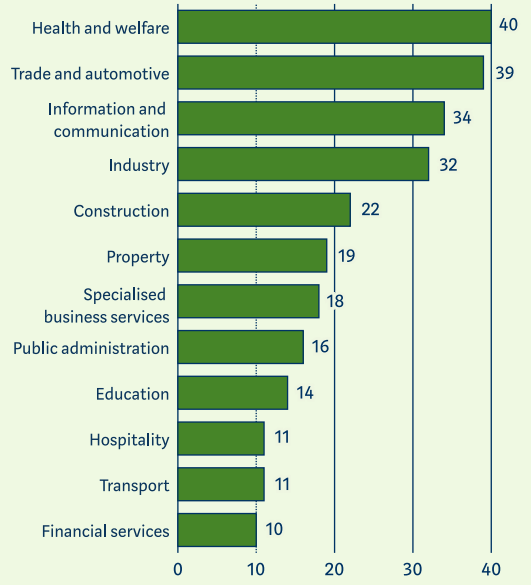


FIGURE 4 | Types of victims affected by a ransomware data breach in 2025

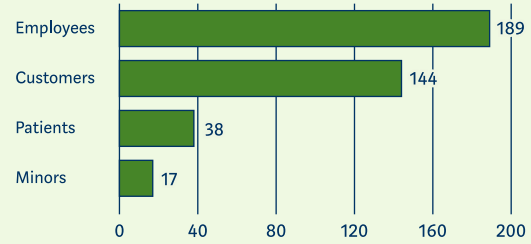


FIGURE 5 | How often each type of personal data was compromised by a ransomware data breach in 2025

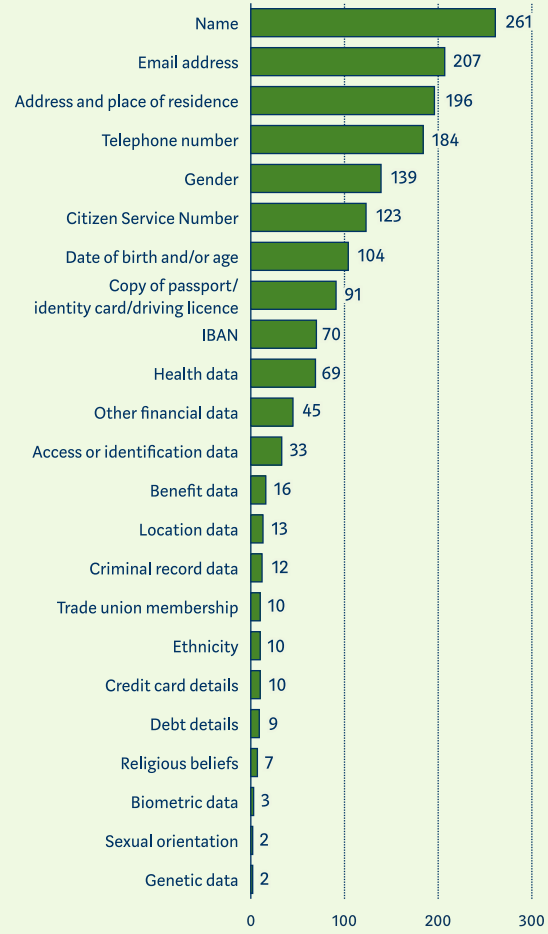
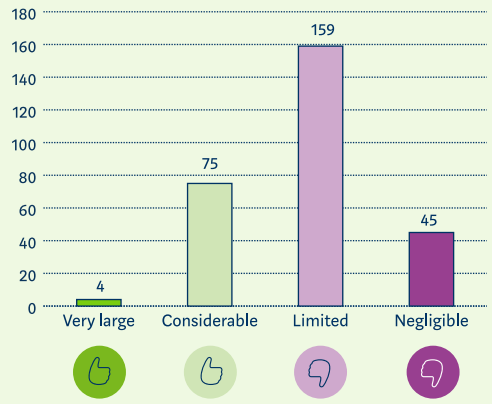


Figure 5 means, for example, that health data is involved in 69 of the reported data breaches. Each data breach could involve the health data of anywhere from tens to hundreds of thousands of people.

Organisations underestimate the risks

Organisations underestimate the risks of a data breach caused by a ransomware attack. As a result, the AP must intervene on a regular basis. For as soon as cyber attackers can access or steal personal data, this almost always poses significant or very high risks to people. Organisations often think that contact details are not considered sensitive data. But if cyber criminals gain access to lists of contact details, they can misuse them for personal scams. Furthermore, organisations frequently believe that if they see no trace of the attack, the risks aren't that great. That is a false assumption: in the event of a cyber attack, an organisation must always assume that the attackers have accessed and stolen data, until log data proves that this is not the case is.

FIGURE 6 | How organisations underestimated the consequences for victims in 2025





2. Experiences of organisations: what to do in the event of ransomware attacks?

Interviews with organisations that have been affected by a ransomware attack

The AP visited a number of organisations that were hit by a ransomware attack and asked about their experiences and lessons learnt. Below are their stories, along with the AP's experiences and tips for organisations to mitigate the impact of ransomware.

1. Discovery
2. Panic or contingency plan
3. Seek help
4. Stay in control of the incident and investigate
5. Communicate
6. Rebuild

1 Discovery: something is wrong

Experience of a wholesaler in the industrial sector:

> During the night, cyber attackers breached the company's network storage. The following morning nothing seemed amiss, at first. One of the employees was unable to log in, which is not uncommon when a password has been forgotten. Shortly afterwards, however, it turned out that nobody was able to log in. The foreign parent company had disabled the VPN tunnel, without explaining why. As a result, nobody was able to work and nobody knew what had happened. This caused a great deal of confusion.
>
> It was only when a piece of paper containing a link to a web page appeared at the printers that the situation became clear. On that page, the attackers were demanding a ransom: the company had been hit by ransomware.

The experience at an online platform in the healthcare sector:

> When building the software, the focus was on speed. So the developer decided not to build any security into the software he was writing. He hoped that hackers would never be able to guess the file names. But of course, they managed to do so, and the attackers were then able to download a large number of files. He was called out of bed: there had been a security incident in which the attackers were demanding a ransom. He knew immediately what had caused this: the poor design choice.

Organisations all discover in different ways that they have become a victim of a ransomware attack. For example, when employees can no longer log in, through their IT supplier, or because the cyber attacker contacts them directly.

Data breach notifications show that cyber criminals often gain access via a technical vulnerability, such as a system that has not been updated (in good time). In addition, cyber criminals often gain access by deceiving people. For example, an employee clicks on a phishing link and enters their login details.

Tip: Make sure there is a good monitoring system in place to detect attacks early and prevent access to your systems.

2 Panic or contingency plan?

Experience of a small international software supplier:

> The ransomware attack was obviously very annoying for the company, but for the professionals of the incident response team, it was also the perfect opportunity to do what they are good at. The IT manager was in his element. He was under a lot of stress, but he also found it exciting and challenging to resolve the attack. He felt that he could finally give it all a thorough clean. Suddenly, everything was possible.

Experience of a software supplier in the transport and logistics sector:

> A few years before the ransomware attack, the company had taken out cyber insurance. Somewhat more recently, the company also attained ISO 27001 certification, a standard for information security. As a result, the company had a plan in place for information security incidents and knew what to do. The company quickly put together a team of specialists to stop the data breach and get the business up and running again as soon as possible.

Organisations respond in different ways following the discovery of a ransomware attack. While some panic, others proceed with an organised plan.

Organisations can save time by thinking ahead about a plan and who does what during a crisis. It also helps to calm employees and provide direction. Moreover, a plan helps with the necessary actions and task allocation to get the computer systems secure and operational again.

Tip: Draw up a plan (on paper) in case your organisation becomes the victim of a cyber attack. Test that plan on a regular basis.

3 Seek help

Experience of a software supplier in the transport and logistics sector:

> The company had made all the necessary preparations, yet it was unable to resolve this attack on its own. The company therefore engaged an incident response team, received support from a law firm and reported the incident to the police, the AP and the National Cyber Security Centre (NCSC).

Experience of a wholesaler in the industrial sector:

> This small organisation did not have the necessary expertise to respond to the incident. However, the team leader did remember that the AP must be notified of all data breaches. In a crisis, this is not only a legal obligation but also helps with the next steps. The AP's data breach form highlights the obligation to provide victims with information about the data breach. He also looked into which personal data within the organisation could have been accessed online. This helped him to get a grip on the attack.

If an organisation falls victim to a cyber attack, it faces a great deal of pressure. There is a high likelihood that the organisation needs help and expertise it does not have. The AP advises organisations to seek assistance from specialist bodies, such as the NCSC, the trade association or an incident response team. It is also a good idea to report the incident to the police.

The AP monitors the protection of personal data. This includes guiding organisations through the steps to be taken following a data breach. The AP's data breach form plays a key role in this: it highlights important considerations and follow-up actions. The organisations that took part in the survey really appreciated this.

AP inspectors may contact the organisation. This happened in 40 of the 136 ransomware attacks investigated. For example, an inspector may provide guidelines or tips on how to provide victims with clear information, or draw the organisation's attention to areas of concern in the investigation.

Tip: Seek help from outside the organisation if you do not have the necessary expertise.

4 Stay in control of the incident and investigate

Experience of an online platform in the healthcare sector:

> Following the discovery of the attack, the first step was to disconnect the infected computers from the internet, ensuring that the hackers no longer had access. Next, the organisation had to investigate whether there were any infected files left anywhere and if the hacker had left a backdoor open. As the organisation was not absolutely sure of this, it decided to rebuild the entire network from scratch.

Experience of a wholesaler in the industrial sector:

> The data breach form asks which data may have been affected by the breach. The IT staff therefore checked which documents were stored in the systems. They found many documents of which it was not clear why they were on the network drive. For example, copies of passports and saved passwords. Many employees also had personal files stored on the company drive. The IT staff immediately deleted these documents.

It is important to get the criminals out as quickly as possible. You also need to understand what happened and which data may have been affected. An organisation must know which personal data it uses and, consequently, which data is stored on the systems. Yet, organisations often only carry out a thorough investigation after an attack.

Sometimes, it does not seem worthwhile for an organisation to invest in an extensive investigation. But if your organisation fails to carry out this investigation, can you be sure that work can continue securely? And how do you inform victims about the risks of the data breach?

Tip: Know which data your organisation stores and from whom. Do not store data longer than necessary, because data you do not have, cannot be breached.

5 Communicate

Experience of a software supplier in the transport and logistics sector:

> The data breach at this supplier also affected customer organisations. Following the cyber attack, the supplier sent them a message explaining what had happened and what the consequences were. When it became clear which data had been stolen, the supplier also immediately informed their customers. This allowed the customers to also investigate to what extent the data breach had affected them. According to the supplier, it was good for the relationship with the customers to report the data breach early and share the details, even if the news was unpleasant. And indeed, the customers appreciated that the supplier was open about the data breach.
>
> The supplier wanted to have as little personal data from customers as possible, because it is unnecessarily risky to manage personal data that you do not need for your work.

It is important to provide organisations affected by the data breach with proper information. In addition, warning messages intended for people who have been affected by a data breach must also be clear and understandable. Victims must be informed of the data breach as soon as possible; additional information from further investigation can be provided at a later stage. If a warning arrives in time, victims can immediately be on their guard against phishing messages or payment abuse, for example.

Sometimes organisations are concerned that they will worry victims by informing them that they have been affected by a cyber attack without having all the answers yet. This investigation shows exactly the opposite.

Tip: Provide the victims with information as soon as possible, so that they can be vigilant right away. For good examples of warning messages, check the AP website.

6 Rebuild

Experience of an online platform in the healthcare sector:

> After the attack, it was clear to everyone in the company where the priority should be. Previously, financial considerations often played a part in security decisions, but after the cyber attack, that was no longer up for debate. Everyone now knows why it is important to keep risks properly under control. And if the IT systems change, we also need to rethink the risks. That is also the advice to organisations with less money for security: tackle the biggest risks first. Focus your attention on what is most likely to go wrong, or where the impact on those affected is greatest.

Once the criminal no longer has access and all the necessary information has been gathered, an organisation needs to get back to work as quickly as possible. The easiest way to do this is by using backups that were not affected by the attack. Sometimes that is not possible, and an organisation needs to rebuild its entire online environment from scratch.

Tip: Ransomware costs organisations a fortune. Invest in a high level of cyber security and start by addressing the biggest risks first. Ensure you have reliable and up-to-date backups.



Paying a ransom offers no guarantees

None of the organisations the AP spoke to has paid a ransom. And that is a good thing, because cyber attackers are not reliable partners.

In 2025, the AP saw cyber attacks in which the organisation did pay a ransom, after which the cyber attackers demanded more money or still went ahead and published the stolen data online. Therefore, the advice remains not to pay. Paying the ransom offers no guarantees and keeps it interesting for criminals to continue carrying out ransomware attacks.

Robust security against data breaches and preparing for when things do go wrong

The tips at a glance:

- Make sure there is a good monitoring system in place to detect attacks early and to prevent access to your systems.
- Draw up a plan (on paper) in case your organisation becomes the victim of a cyber attack. Test that plan on a regular basis.
- Seek help from outside the organisation if you do not have the necessary expertise.
- Know which data your organisation stores and from whom. Do not store data longer than necessary, because data you do not have, cannot be breached.
- Provide the victims with information as soon as possible, allowing them to be vigilant right away. See the examples of warning messages on the AP website.
- Ransomware costs organisations a fortune. Invest in a high level of cyber security and start by addressing the biggest risks first. Ensure you have reliable and up-to-date backups.

In addition:

- Data minimisation & retention periods: do not collect more data than necessary and not for too long. Data you do not have, cannot be breached.
- Basic principles for digital resilience (NCSC). With the basics in place, many ransomware attacks can be prevented.



De Autoriteit Persoonsgegevens is de onafhankelijke toezichthouder op persoonsgegevens die mensen beschermt in een digitale wereld.

Autoriteit Persoonsgegevens
Postbus 93374
2509 AJ Den Haag

autoriteitpersoonsgegevens.nl