Ransomware report

Inadequate security made two out of every three affected organisations vulnerable

Report for October 2024

AUTORITEIT
PERSOONSGEGEVENS

Table of contents

1. Summary

Organisations insufficiently able to defend themselves against ransomware because of inadequate security

In 2023, 178 unique ransomware attacks were reported to the Dutch Data Protection Authority (Dutch DPA). An investigation carried out by the Dutch DPA shows that the basic security was not in order at two out of every three affected organisations. That is why the Dutch DPA calls on organisations to get their basic security in order, to be able to defend themselves against ransomware.

Basic security in order

The Dutch DPA calls on organisations to take in any case the following measures:

1. implement multifactor authentication (MFA).
   And enforce its use among employees;
2. formulate a good password policy;
3. carry out updates in time. Especially in the case of known vulnerabilities (such as 'Common Vulnerabilities and Exposures' or CVEs);
4. ensure sufficient network segmentation.

New trend: privacy victims suffer extra harm from double extortion

In around 50% of the ransomware attacks investigated, cyber criminals did not only encrypt systems, but also stole (personal) data. This is extra harmful for the privacy of the people concerned, because their data may end up on the dark web. Moreover, this increases the risk of identity fraud, phishing and other types of fraud.

Not paying is the standard

The investigation of the Dutch DPA shows that around 9% of the organisations investigated decide to pay a ransom after a ransomware attack. However, paying a ransom is not a solution or a security measure. It gives no guarantee that leaked personal data will not be sold or published all the same. Besides, it allows crime to continue. That is why not paying is the standard.

The investigation

Personal data are involved in many ransomware attacks. This may result in high risks for the victims. They may receive phishing mails or become the victim of identity fraud. Because of the high risks, organisations are nearly always obliged to report this type of data breaches to the Dutch DPA and to the victims. Thanks to this notification obligation, the Dutch DPA has gained a broad picture of the nature and size of ransomware attacks in the Netherlands.

More insight in ransomware attacks helps Dutch society withstand them better, which is beneficial to the protection of personal data. For this investigation, the Dutch DPA analysed the incident reports, data breach reports, email exchanges, data breach registers and technical details of 90 ransomware attacks.

2. Basic measures are not in order

Two out of every three organisations affected by ransomware did not have the basic security in order. As a result, they were insufficiently able to withstand a ransomware attack. The Dutch DPA is very worried about the level of security of the organisations investigated. The four most important missing aspects of basic security are:

1. Implementation of multifactor authentication (MFA);
2. strong password policy;
3. adequate response to generally known vulnerabilities (also called 'Common Vulnerabilities and Exposures' or CVEs);
4. sufficient segmentation of the network.

This chapter is about 63 of the 90 attacks investigated. This is because for the other 27 incidents it was not clear which vulnerabilities were used by the cyber criminals to obtain access.

2.1 Multifactor authentication (MFA) missing

In 52% of the cases investigated, it was explicitly stated that MFA had not been enabled or enforced at the affected organisation. This does not mean that MFA was in order at the other 48%, only that it was not explicitly mentioned there that MFA was missing. The number of successful attacks where MFA was not enabled is probably higher than the 52% emerging from this investigation.

The Dutch DPA finds it to be worrying that even now, MFA is not a standard part of the cybersecurity policy of some Dutch organisations. All the more so because in the Data Breaches Report 2020, the Dutch DPA already paid attention to how MFA can reduce the impact of a data breach or even prevent a data breach.[1]

What is MFA?

MFA means that two or more 'factors' must always be used to log in: something that you know (a password, for example), something that you have (a temporary code sent through an app, for example) or something that is part of you (a fingerprint, for example)[2]. This measure is relatively cheap and easy to implement. This is why organisations increasingly use MFA. Logging in with an extra step gives users a lot of extra protection.

2.2 Bad password policy

The second basic measure that organisations still do not have sufficiently in order is the implementation of a good password policy. This is worrying too, given that the Dutch DPA already paid extensive attention to this in a guide from 2021.[3]

How strict a password policy has to be varies for every organisation. There are minimum requirements that every organisation should have to meet, though. Of the 63 organisations investigated, 15 did not meet these requirements. Bad password policy was explicitly mentioned here as a reason for the success of the ransomware attack or for the impact of the attack. For example, the same password was used for all admin accounts. The people who use the systems also have to create and use a strong password. At an earlier time, the Dutch DPA already gave tips about strong passwords.[4] In combination with MFA, strong passwords can prevent a considerable part of the ransomware attacks.

2.3 Updates not carried out in time

The third basic measure that was missing at the organisations investigated was carrying out updates in time, specifically where it concerned updates that counter a 'Common Vulnerability and Exposure' (CVE).

If organisations do not carry out updates soon enough after a CVE becomes known, they are extra vulnerable to ransomware attacks. This proved to be the case for 8 of the 63 organisations investigated. In 6 of these cases, solutions for the vulnerabilities, the 'patches', had already been known for more than one month. Several vulnerabilities of more than one year old also emerged from the investigation. The software, and the organisation with it, had therefore already been vulnerable for more than a year, despite the fact that the update was available.

What are Common Vulnerabilities and Exposures (CVEs)?

If a CVE has been established, a software provider, governmental organisation or independent researcher shares a vulnerability online with the aim of alerting organisations to it. This enables organisation to mitigate the vulnerability where possible, for example by carrying out updates. Because this information is shared online, cyber criminals also have access to it. They can use the information for a ransomware attack. Swift action is therefore of the essence for organisations.

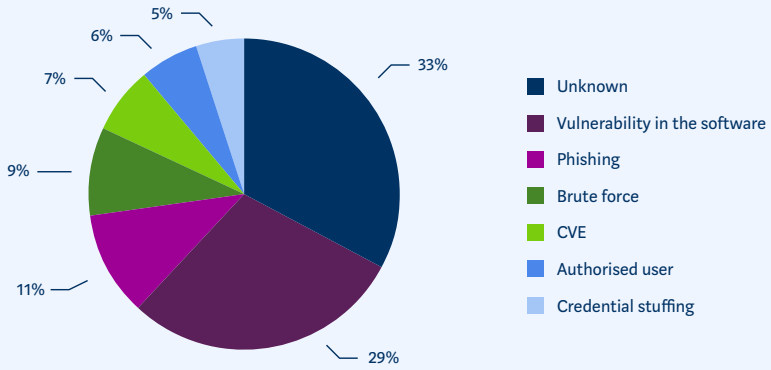
First point of access to the systems ('initial access')

As can be seen in Figure 1, there were several ways in which cyber criminals obtained access to the systems of the organisations investigated. This first point of access to systems is also called 'initial access'.

A common way to obtain access is through a vulnerability in the software. In some cases, it could be established that this was caused by a CVE. In this investigation, CVEs were defined as vulnerabilities that had been known for more than one month and had not been solved.

On several occasions, criminals obtained access through an existing account at the organisation. This is possible, for example, by means of 'credential stuffing': using login details that were leaked earlier. And criminals use 'brute force' attacks when they use computer programmes to try out (random) login details to obtain access to the systems. If none of these techniques could be established, but access had been obtained by logging in with known details, this is classified in the figure under the category 'authorised user'.

FIGURE 1



Which personal data?

Figure 2 shows which types of personal data were leaked during a ransomware attack and how often this happened. It is striking that name, address, telephone number and email address are leaked in almost every attack. In addition, it is very worrying that in 75% of the cases, copies of ID documents and passports got into the wrong hands, resulting in a higher risk of identity fraud.

FIGURE 2

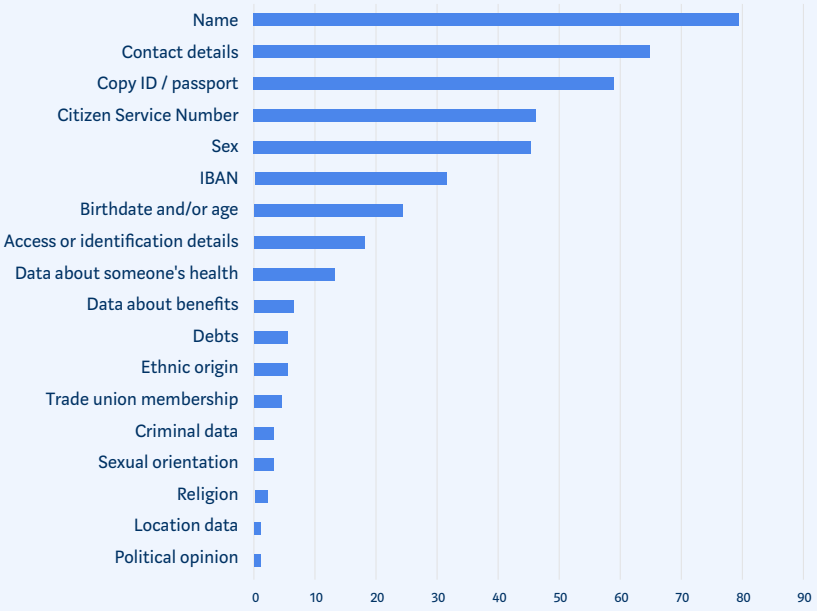


Figure 2 relates to 79 of the 90 organisations. At the other 11 organisations, there was a substantial variation in the types of personal data that were leaked.

2.4 Little to no network segmentation

The fourth and last basic measure that was not in order at the organisations investigated is the lack of (sufficient) network segmentation. This was the case at 12 of the 63 ransomware attacks.

Network segmentation is a security measure with a delaying effect. The longer the cyber criminals are busy performing 'strange' actions in the network, the higher the chance that the security software or a system administrator notices this and can (partly) prevent the attack. At several organisations, network segmentation appeared to be the reason why cyber criminals could only encrypt part of the network. Besides, network segmentation increases the chance of backups remaining available, enabling an organisation to get back to work quickly. In addition, the organisation will not have to make the difficult assessment of whether or not to pay to regain access to the systems.

What is network segmentation?

Network segmentation means that not the entire content of a network is located in the same place. Data have been distributed over multiple servers that have been physically separated from each other or by means of a digital security layer (e.g. a firewall). This distribution makes it much more difficult for cyber criminals to obtain access to certain 'rights' in the system that they can use to encrypt the entire network. The more difficult this is and the more time it takes, the greater the chance of being caught and the less valuable the loot.

3. New trend: double extortion

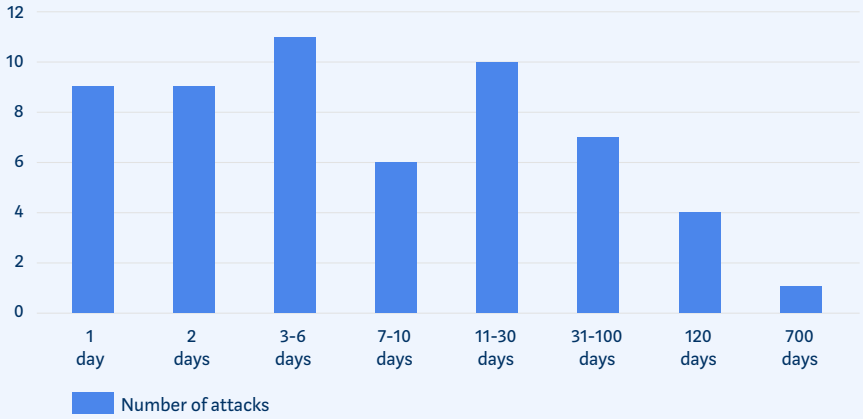
A new trend can be discerned in the Netherlands: double extortion. In around half of the attacks investigated (44 out of 90), the organisation was not only affected by ransomware – after which a ransom was demanded – but the cyber criminals also stole data. In addition, at least 8 other organisations suspected that this had happened. The cyber criminals threatened to publish or sell the stolen (personal) data if the organisation did not pay.

The data that are stolen by the cyber criminals are often personal data. Double extortion therefore results in a double risk for the people whose data were affected. Not only do the cyber criminals steal data; they subsequently publish or sell the data on the dark web as well. The danger is in particular great if stolen data are combined with each other. Where a single data may sometimes not mean much, a combination of data may result in a detailed profile of an individual. Criminals use such profiles for targeted phishing mails or identity fraud. In 2023, more than 7000 people reported identity fraud to the Central Identity Theft and Error Reporting Centre (CMI)[5].

How long were they in?

Figure 3 shows how long the cyber criminals were in the network of the affected organisation. This is the period between the first time the cyber criminals were clearly active on the network and the time the cyber criminals encrypted the network. In some cases, this was a relatively short period, without the cyber criminals being active in the meantime. In the case of the outliers on the right side of the chart, for example, the cyber criminals were not constantly busy for two years, but they did not look at the organisation for a period after the initial access. Not until a (much) later time did they proceed to encryption. In those cases, organisations therefore had a lot of time to notice the hack and prevent further damage.

FIGURE 3

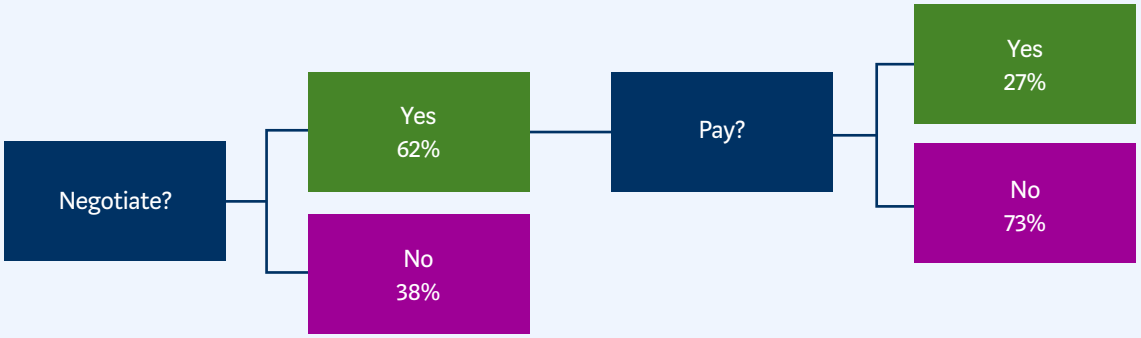


4. Not paying is the standard

Of the 90 organisations investigated, at least 8 paid a ransom to the cyber criminals (Figure 4). The Dutch DPA feels that it is a good thing that the vast majority of organisations do not pay a ransom. After all, paying allows an illegal system to continue. The less often organisations decide to pay after a ransomware attack, the less attractive the Netherlands becomes for cyber criminals. This is beneficial to the protection of personal data of Dutch people.

Besides, payment is no guarantee that the cyber criminals will keep their word. In this investigation, the Dutch DPA saw that an organisation did not regain access to the systems after payment, despite the promise from the cybercriminals. The system remained encrypted, and the stolen (personal) data nonetheless ended up on the dark web. The cyber criminals had disappeared without a trace.

FIGURE 4



Negotiate and pay?
Figure 4 shows what organisations do after discovering a ransomware attack. Organisations have the choice to contact or not to contact the cyber criminals, and to pay or not to pay. The majority of organisations contact the cyber criminals to find out what they have stolen. After that first contact, often through a private connection on the dark web, most organisations decide not to pay. Of the 62% who decide to negotiate, 27% eventually pay.

5. Sources

1. Data breach notification obligation annual report 2020 | Dutch Data Protection Authority
2. Tech blogpost: factors in authentication | Dutch Data Protection Authority
3. EDPB guidelines on examples regarding personal data breach notification
4. Tech blogpost: strong passwords in practice | Dutch Data Protection Authority
5. Figures: Central Identity Theft and Error Reporting Centre (CMI) | National Office for Identity Data (RvIG)

AUTORITEIT
PERSOONSGEGEVENS