LIFELINE

Protect your network against cybercrime

Practical tips and a checklist for protecting your external data connections

eurofiber

Contents

Is your WAN GDPR-proof?

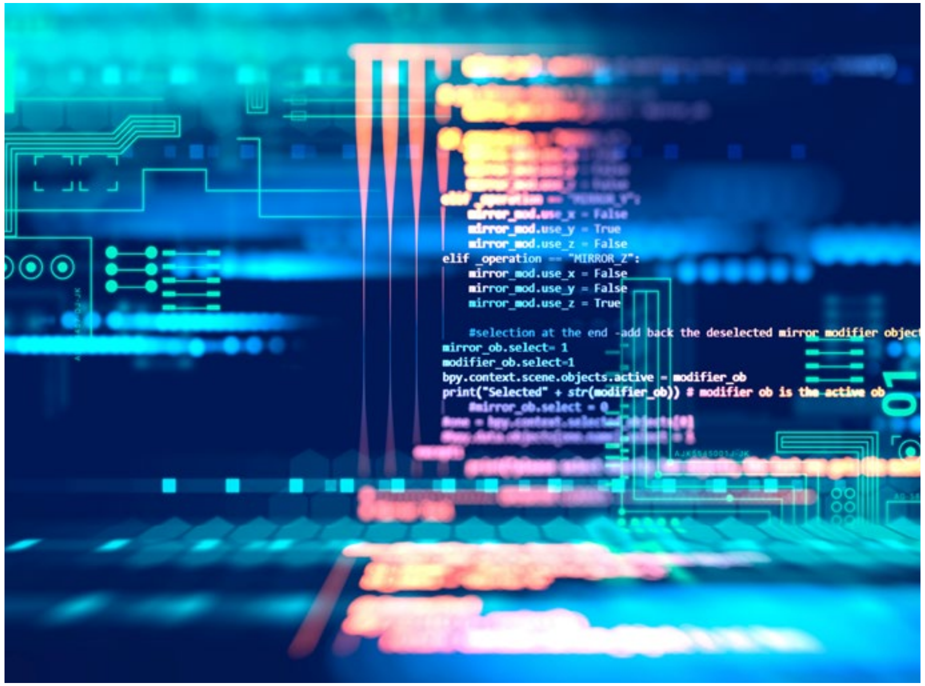
In this eBook, we will explain the vulnerabilities in WAN, the possible consequences of a data breach, and what you can do to protect your data connections.

With the implementation of the General Data Protection Regulation (GDPR), the government imposes strict requirements on the way your organization processes personal data. Within the walls of your own organization, you can take steps to protect your privacy-sensitive data. Outside that, your data is only as secure as the protection that the Wide Area Network (WAN) provides. Due to the emergence of the cloud (public, private or hybrid), data constantly shifts between organizations and data centers. Your data also needs to be protected effectively 'in transit'. Many organizations assume that managed services are protected at the proper level by default. That is not the case.

Managed connections also need to be secured. It is absolutely vital to encrypt your data and take control of your key management.

What do laws and regulations say about your WAN connections?

The mandatory notification in case of data breaches as well as the GDPR are forcing organizations to take an even more critical look at their network connections. In addition, the network connections of organizations need to comply with sector-specific certifications, such as NEN7510 (healthcare sector) and BIR (government). The European Agency for Network and Information Security (ENISA) advises:
WAN connections always need to be encrypted, since it is difficult to guarantee the physical safety of connections across Wide Area Networks, including public and private fiber optic cables. In practice, WAN connections are by no means always encrypted, because many companies assume incorrectly that the nature of fiber optics always provides sufficient protection.



```
elif _operation == "MIRROR_Y":
    mirror_mod.use_x = False
    mirror_mod.use_y = True
    mirror_mod.use_z = False
elif _operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True

    #selection at the end -add back the deselected mirror modifier object
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the active ob
    #mirror_ob.select = 0
```

Fiber optics can also be a target

Where possible, organizations choose fiber optic connections to connect their locations and data centers. If that is also the case for your organization, then you need to be alert to potential hazards. Fiber optic connections have a solid reputation for speed, reliability and security, but cyber criminals could tap into fiber optic cables, for instance in parking garages and locations where the fiber connection comes out of the ground. Using a special clip called a fiber tap, malicious parties can imperceptibly intercept light pulses from the fiber optic line and steal emails, phone calls and other data. With a bit of bad luck, this tap will go completely unnoticed, resulting in a serious data breach. Even if you have protected the rest of your IT infrastructure perfectly, it still does not mean that your WAN is automatically protected as well as you need it to be.

A survey* amongst IT decision-makers has shown that less than half (47%) of the respondents are checking their WAN connection in the context of privacy legislation and security. A quarter of the people who responded indicated that the security of the rest of the IT infrastructure has been handled properly, which means that their WAN connection does not need any additional attention. These results are cause for concern, as this does not guarantee that the connections between offices and data centers are actually secure. In other words, many organizations run a real risk of having a data breach, resulting in huge fines and damage to their reputation.

* Source: White paper by Telindus

GDPR fines

An incident is considered a data breach when sensitive, insufficiently encrypted personal data (such as login details, citizen service numbers, or financial and medical data) has been lost or is no longer available. In the event that a data breach occurs and data is not protected according to the statutory regulations, the fines could be steep:
If an organization is in violation of the General Data Protection Regulation (GDPR)then the Data Protection Authority can impose a fine of up to 20 million euros or 4% of the company's annual turnover, whichever is highest. There are two categories of GDPR violations and accompanying maximum fines:

Maximum fine of 10 million euros

Data processors (organizations that process personal data) are subject to certain obligations under the GDPR, such as the documentation requirement. If a data processor does not comply with one or more of these requirements, the Data Protection Authority can impose a fine of a maximum of 10 million euros – or a fine of 2% of the annual global turnover, if that amount is higher.

Maximum fine of 20 million euros

If a data processor violates the core principles or foundational concepts of the GDPR, or the privacy rights of the people involved (the people whose information is processed by the organization), the Data Protection Authority can impose a fine of a maximum of 20 million euros – or a fine of 4% of the annual global turnover, if that amount is higher.

* Source: Dutch DPA

Example of damage due to unauthorized access

Hackers gained unauthorized access to data on the network of a group of schools. The incident was the result of an unknown vulnerability. The information included contact details and financial data of teachers and students. The total costs amounted to € 282,100. This included the costs of forensic investigation and legal defense costs related to claims for privacy liability.

(Source: VMD Koster insurance group).

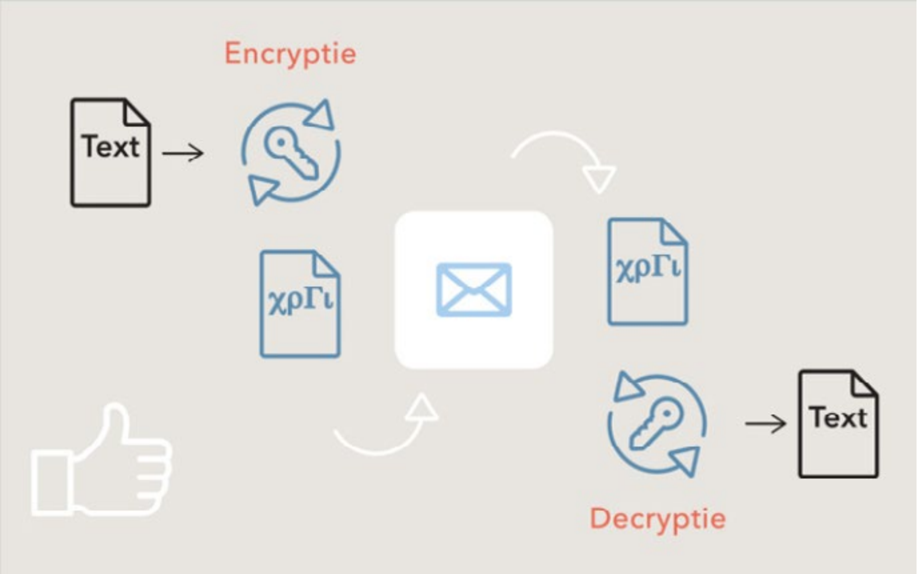
What can you do?

As discussed above, ENISA has stated that WAN connections should always be encrypted. Data encryption on the IP and Ethernet layer is complex and expensive, and will decrease the performance of your connections. Key management is very difficult. That means that the ENISA guidance will pose a challenge for many organizations. Research has shown that a good 65% of organizations outsource management of their fiber optic lines, and therefore also the security of those connections. The benefit is that organizations theoretically have little to worry about regarding external connections. There are also drawbacks, however. A leased fiber optic line is relatively expensive, if you will only be using the fiber connection for a single application. Moreover, with the current GDPR it is no longer certain whether the WAN connections have been protected to a sufficient extent. Every IT decision-maker faces the challenge of thoroughly scrutinizing their WAN, assessing security, and determining whether outsourcing IT security management is their best choice.

Checklist: is my WAN GDPR-proof?

Ask yourself (or your external provider) the following questions to find out if your WAN is sufficiently protected against data breaches:

- ☐ Is my data and my clients' data available at all times? No? If the data center is not available, that is considered a data breach.
- ☐ Is my data center entirely redundant (active/active, geographically separated)? No? Failure of a single data center (or connection to the data center) causes a data breach, and must be notified to the authorities.
- ☐ Is the redundancy implemented correctly? That means that the lines are physically separated down to the device level. It may seem better to partner with two dark fiber providers. However, that is not the case in practice, as two different providers will not coordinate to align any work activities or overlaps in physical lines. Without such coordination, the risk of failure becomes a realistic possibility. For that reason, it is advisable to source redundant connections from a single provider.
- ☐ How are my connections performing: are they fast enough, are they scalable, and what bottlenecks have been identified?
- ☐ What is the SLA's position on damage to the fiber optic connection and how fast it will be repaired?
- ☐ What type of protection is provided on the connections?
- ☐ How are my encryption keys managed?



A well-kept secret: WDM with optical encryption

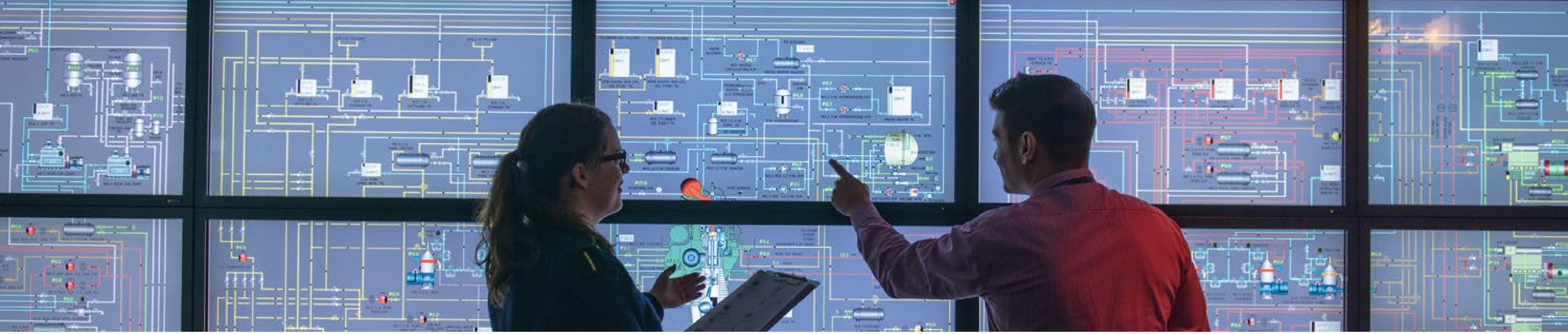
VResearch shows that only 22% of all IT decision-makers manage their fiber optic connections within their own organization. Other IT decision-makers do not see the need for it (33%), do not have sufficient manpower (18%) or knowledge (13%) in-house, or view the investment costs as an obstacle (11%). If you are part of the majority that outsources everything, it is worth the effort to explore the alternative.

Wavelength Division Multiplexing (WDM) combined with optical encryption provides a safe and easy way to manage the WAN connections within your own organization. This relatively less well-known but effective technology is a cost-efficient alternative to ensure that your WAN complies with GDPR requirements, as well as with the NEN7510 and BIR standards referenced

above. The technology also complies with the highest level of IT security guidance for Transport Layer Security, as described by the National Cyber Security Center.

What does WDM do?

WDM makes it possible to transport data over eighty channels across long distances. The technology relies on a single fiber pair to route multiple information streams at the same time. In practice, that means that multiple signals or colors can be sent at various wavelengths across one single fiber optic connection. WDM eliminates the need to have a separate line for each connection, which significantly reduces complexity and costs. Using WDM makes it possible to transport terabits of data across a single fiber pair. This approach allows you to multiply your bandwidth and achieve huge savings on leasing fiber optic lines or managed connections.



The 5 benefits of WDM in conjunction with optical encryption

When implementing WDM connections, data can be encrypted in the optical layer itself. This type of encryption has the following benefits compared to the most common type of encryption on the IP or Ethernet layer:

1. Operational simplicity

A good encryption solution in the optical layer is always active. This means that WAN traffic is guaranteed to be protected, regardless of any configuration in higher layers. This approach eliminates any human errors. By using the X.509 protocol, the security officer can sign security certificates for authentication with his PKI (Public Key Infrastructure), ensuring that encryption keys and root certificates remain with the security officer. They do not need to be shared with the network manager, integrator or managed services provider. The security of the solution is guaranteed by external certification: FIPS 140-2 Level 2 hardware certification and FIPS-197 AES-256 certification are absolutely vital, offering guarantees for a secure solution.

2. High bandwidth, low latency

Transmission and encryption take place in the hardware. Optical encryption only adds 5 microseconds of latency to the connection. In comparison: encryption in the IP layer involves milliseconds of latency, increasing delay by a factor of 1,000.

3. Transparency and flexibility in protocols

The connections between data centers are often a combination of various transmission speeds and protocols (100GbE, 40GbE, 10GbE, Fiber Channel, OTN). WDM cards (transponders) with encryption are transparent and protocol-independent. That makes them suitable for Ethernet, SDH, OTN and Fiber Channel Transport.

4. Simpler management

WDM with encryption is basically transport and security in one single device, which is good for operational costs: just one support contract, one training course, and one single investment in spare parts, instead of two or more sets of parts.

5. Cost reductions

The use of WDM technology in conjunction with encryption achieves huge savings on optics in the routers and switches. It also reduces energy use by 60% and requires 50% less in connections and equipment.

Business case: WDM with optical encryption

In many cases, the benefits will outweigh the familiar obstacles, such as insufficient manpower, knowledge and budget. In virtually all cases, the use of WDM in conjunction with optical encryption will result in a favorable business case and a quick return on investment.

In case of managed WDM services, the service provider takes on everything related to implementation and transport management, while you retain control of the encryption keys. It is not advisable to make huge investments in training and personnel in order to get the maximum results from WDM technology. A WDM solution including encryption requires a far smaller number of changes per year than a data center or Campus LAN environment, so the gains from investing in knowledge for your own staff are significantly smaller. Many organizations will therefore be better off by opting for Managed Services. This hands-on example shows how fast you can achieve returns on your investment:

Data center Explore your options

To safeguard the security of your data and to avoid high fines and reputational damage, you need to take a closer look at your external connections. That level of scrutiny still remains relevant if you outsourced the lighting and management of your fiber optic lines. That is certainly not an easy job, but it will result in a safe and future-proof network. The checklist in this e-book will help you take stock of your situation, and Eurofiber would be happy to advise you. Also keep in mind that WDM Encrypted in the optical layer of a Eurofiber connection provides a suitable alternative to optimize your WAN connections, making them easier to manage, as well as GDPR-proof.

Curious to hear more about what we could achieve for your organization?

Eurofiber has been a fast-growing international provider of industry-leading digital infrastructure since 2000. Relying on our own fiber optic network and data centers, we provide smart, open, future-proof infrastructure to companies, government bodies and non-profit organizations. Customers have complete freedom to choose the services, applications and providers they need, allowing them to tap into the full potential of digital innovation. Eurofiber has an extensive fiber optic network in the Netherlands and Belgium, it unlocks its four data centers of its own and almost all public data centers in the Benelux.

This is a Lifeline eBook brought to you by Eurofiber. The Lifeline platform offers information and inspiration in the field of digital connectivity. Eurofiber.be/lifeline.

Eurofiber. Lifeline for the digital society

Fountain Plaza 504, Belgicastraat 5 bus 7,
1930 Zaventem, t +32 (0)2 307 12 00
info@eurofiber.be, www.eurofiber.be

eurofiber