THE POWER OF BEING UNDERSTOOD

AUDIT I TAX I CONSULTING

IT INSIGHTS

CYBERSECURITY: HOW DOES YOUR COMPANY AVOID CYBER ATTACKS?

RSM

As you probably noticed the number of cyber attacks has increased the recent months. Last weekend the residential care centre in Willebroek was the target and earlier this month the manufacturing company Picanol was severely impacted.

Asco is still recovering from the cyber attack in June 2019. At that time, the manufacturer of aircraft parts did not accept to pay the ransom and chose to solve the problem itself. The recovery of the affected production systems is still in progress after 6 months. This has serious financial and reputational consequences for Asco.

In response to these various cyber attacks, we would like to share a few **best practices** to prevent cyber attacks on your company’s infrastructure.

- Implement **multi-factor authentication** to login.
- Block **mail forwarding** so that hackers cannot forward and read sensitive information.
- Monitor unsuccessful login attempts and automatically block the Office 365 account after e.g. 5 unsuccessful attempts.
- Regularly check the error messages in the Office 365 administrator account

In addition to this specific configuration, we recommend you to:

- Regularly test your IT systems for possible security risks and vulnerabilities e.g. by an ethical hacker.
- Continuously train your staff by providing **awareness** training on **phishing, ransomware, etc.** The root cause of a successful cyber attack is often a human error.
- Minimize the use of mobile devices e.g. USB sticks, external harddrives, memory cards, etc
- Limit **single sign on (SSO),** especially to access business critical systems.
- Isolate critical machines in a separate VLAN with limited or no access to the Internet or internal network.
- Make sure all systems e.g. Firewall, PC's,... have the latest security updates.
- Use preferably an anti-virus that has "**containerized**" capabilities so that email attachments are not opened locally, but by default in the **cloud**. **Ransomware** will be less likely to spread locally in your network.
- Make sure to have a cyber insurance to partially cover your financial risks.

If you need help with the implementation of the above topics, do not hesitate to contact RSM IT Advisory.
Ask for our free brochure on **penetration testing** of your website, **Ethical Hacking** and 24/7 **Treath Detection & Response Services.**

RSM IT Advisory regularly organizes workshops on Digital Transformation, Cyber Security and GDPR, click here to subscribe to our newsletter so you are informed about the next workshop.

RSM Belgium souhaite, par ce document, fournir des informations générales, sans que les informations contenues dans ce document ne soient considérées comme un avis. La rédaction s’efforce de composer cette édition de la manière la plus précise possible. Cependant, nous ne pouvons pas vous garantir que ces informations seront toujours exactes au moment où elles seront reçues ou qu’elles seront toujours exactes dans le futur.

You can already register for our Cyber Insurance workshop at itadvisory@rsmbelgium.be

CONTACT DETAILS:

Steven VERMEULEN
Partner IT Advisory
s.vermeulen@rsmbelgium.be
✆+32 494 51 86 03
☎ +32 3 449 57 51

RSM Belgium souhaite, par ce document, fournir des informations générales, sans que les informations contenues dans ce document ne soient considérées comme un avis. La rédaction s'efforce de composer cette édition de la manière la plus précise possible. Cependant, nous ne pouvons pas vous garantir que ces informations seront toujours exactes au moment où elles seront reçues ou qu'elles seront toujours exactes dans le futur.

ZAVENTEM
Lozenberg 22 b 2 - B 1932 Zaventem
T +32 (0)2 725 50 04 - F +32 (0)2 725 53 41

ANTWERP
Posthofbrug 10 b 4 - B 2600 Antwerp
T +32 (0)3 449 57 51 - F +32 (0)3 440 68 27

BRUSSELS
chaussée de Waterloo 1151 - B 1180 Brussels
T +32 (0)2 379 34 70 - F +32 (0)2 379 34 79

CHARLEROI
rue Antoine de Saint-Exupéry 14 - B 6041 Gosselies
T +32 (0)71 37 03 13 - F +32 (0)71 37 01 39

MONS
boulevard Sainctelette 97 b - B 7000 Mons
T +32 (0)65 31 12 63 - F +32 (0)65 36 37 07

AALST
Korte Keppestraat 7 bus 52 - B 9320 Erembodegem
T +32 (0)53 75 12 20

interaudit@rsmbelgium.be
interfiduciaire@rsmbelgium.be
intertax@rsmbelgium.be
interpay@rsmbelgium.be
itadvisory@rsmbelgium.be

WWW.RSMBELGIUM.BE

RSM Belgium is a member of the RSM network and trades as RSM. RSM is the trading name used by the members of the RSM network.

Each member of the RSM network is an independent accounting and consulting firm, each of which practices in its own right. The RSM network is not itself a separate legal entity of any description in any jurisdiction.

The RSM network is administered by RSM International Limited, a company registered in England and Wales (company number 4040598) whose registered office is at 50 Cannon Street, London, EC4N 6JJ.

The brand and trademark RSM and other intellectual property rights used by members of the network are owned by RSM International Association, an association governed by article 60 et seq of the Civil Code of Switzerland whose seat is in Zug.

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM