
CYBER IN E-COMMERCE:
HOW TO SECURE YOUR WEBSHOP?
feweb

DIGITALIZE & FEWEB

DEZE PRESENTATIE BEVAT DE EXPERTISE VAN DEZE BEDRIJVEN:

BUCKAROO

ESIGN

eye cyber security

Groovix

marcando

make it fly

METEOR

SIRIUS.LEGAL
BUSINESS LAW FIRM

stellar lab

se studio emma
internet expertise

PrestaShop: +300.000 online shops attacked by SQL-injection

Nieuws

Webwinkels aangevallen via zerodaylek in e-commerceplatform PrestaShop

dinsdag 26 juli 2022, 10:57 door **Redactie**, 1 **reacties**

Criminelen maken misbruik van een combinatie van bekende en onbekende kwetsbaarheden in e-commerceplatform PrestaShop om webwinkels **aan te vallen** en te voorzien van malafide betaalpagina's die creditcardgegevens van klanten naar de aanvallers sturen. Zo'n 300.000 webshops wereldwijd draaien op PrestaShop.

Door middel van onder andere SQL Injection kunnen de aanvallers willekeurige code uitvoeren op de servers waarop de PrestaShop-webwinkel draait, zo stelt het ontwikkelteam. Bij de nu waargenomen aanvallen gebruiken de aanvallers de kwetsbaarheden om klantgegevens waaronder creditcarddata te stelen. De beveiligingslekken zijn aanwezig in PrestaShop 1.6.0.10 en nieuwer. Versie 1.7.8.2 en nieuwer zijn niet kwetsbaar, tenzij ze een module of custom code draaien die wel kwetsbaar is. Versies 2.0.0~2.1.0 van de Wishlist (blockwishlist) module zijn ook kwetsbaar.

Volgens PrestaShop maken de aanvallers gebruik van een onbekende "vulnerability chain" voor het uitvoeren van de aanval, waarbij ze mogelijk de MySQL Smarty cache storage features als onderdeel van de aanval gebruiken. Inmiddels heeft PrestaShop **versie 1.7.8.7** uitgerold die de MySQL Smarty cache storage tegen het injecteren van code moet beschermen.

Het PrestaShop-ontwikkelteam roept alle webwinkels op om de update te installeren, maar stelt ook dat niet kan worden uitgesloten dat de aanval ook op andere manieren is uit te voeren. Daarnaast doet de update vermoedelijk weinig voor webshops die al zijn gecompromitteerd. Verder laten de ontwikkelaars weten dat de MySQL Smarty cache storage een legacy feature is die in toekomstige versies van het e-commerceplatform wordt verwijderd.

Anne Masson

CEO | Eye Security Belgium

During her career, Anne switched from insurance to tech. She has been in charge of expanding Eye Security in Belgium for the past year. She is a passionate team player who likes to combine her sales skills and experience in risk management and technology with entrepreneurship to put Eye Security Belgium on the map.

CONTENT

- About Eye Security
- Threats in E-Commerce
- IRP – Incident Response Plan
- Process Steps
- Importance of Preparation
- Services

About Eye Security

Eye Security is an insurtech company that makes cybersecurity accessible to European companies. With a growing team of security and insurance experts, Eye Security offers a high-quality all-in-one security product, including cyber insurance.

Eye Security is a pioneer in the European market in offering a data-driven solution combining high-quality technology, human expertise and cyber insurance.

Cyber Threats in E-commerce

- **Financial Fraud**
- **Credit Card Fraud**
- **Phishing**
- **Spamming**
- **DoS & DDoS Attacks**
- **Malware**
- **SQL Injection**
- **....**

Cyber-security is very important if you are to succeed online. Hackers are improving their games, so you need a dedicated team to stay updated with security issues and provide your digital infrastructure with around-the-clock protection.

A cyber attack can significantly impact your company's business operations.

It is, therefore, essential to draw up, practice and improve a good Incident Response Plan (IRP), Cyber Disaster Recovery Plan (CDRP) and Cyber Business Continuity Plan (CBCP).

CDRP

A CDRP is focused on recovering the IT infrastructure after a cyber incident. The goal is to restore the systems and applications as quickly as possible and to resume business operations. The ***CDRP focuses on the technical aspects*** of the IT infrastructure and often has a shorter Recovery Time Objective (RTO) than the CBCP.

CBCP

A CBCP is focused on maintaining business operations' continuity, even during a cyber calamity. It's designed to keep the essential business processes running and to minimise the impact of the failure of critical systems on business operations. The ***CBCP focuses on the business processes*** and often has a longer recovery time objective (Recovery Point Objective, RPO) than the CDRP.

Process Steps

01 **Capabilities:** Write down your strengths and weaknesses and know what security measures have already been taken.

02 **Helplines:** Know the existing helplines and make sure they are available in case of a cyber incident. In case of doubt, always contact Eye Security's Incident Response Team.

03 **Crisis Organisation:** Make internal agreements about when escalation to the crisis organisation will occur.

Process Steps

04 **Legal Department:** Know which authorities to notify during a hack or data breach.

05 **Communication:** Think about how you will communicate if the company network fails.

06 **Business Continuity:** Develop alternatives to ensure business continuity. Determine which systems in your network are most important.

07 **Insurance:** Write down the financial consequences of a cyber attack on your company or organisation. Check whether you are insured for this and to what extent you meet the policy conditions.

Why is preparation so necessary?

Because the question isn’t whether you will become a victim of a cyber attack but when!

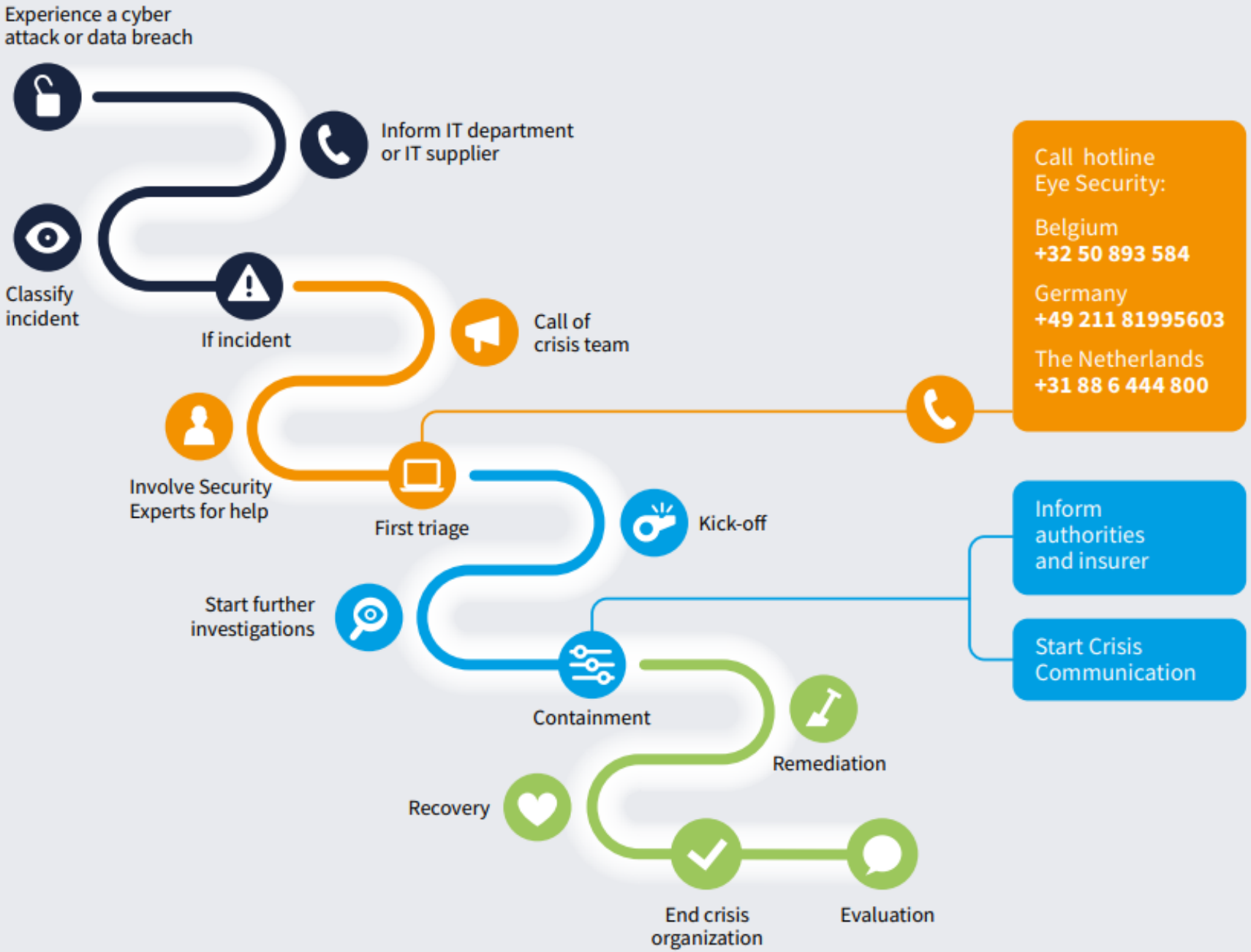
We call this the **assume breach assumption**: assume that you will be attacked because you will. In many cases, intruders access your company systems through a clicked phishing link. Human errors remain by far the weakest link in your cyber defence.

Even when employees are aware and trained to recognise phishing emails, a mistake can happen in a split second: a moment of distraction, hurry or confusion. And this one click can have major consequences for your business operations and its continuity.

GET YOUR COPY

AT BOOTH 1005 OR

DOWNLOAD VIA QR



Managed XDR

24/7 MONITORING

Eye Security closely monitors threats to your office network and cloud environment, meaning your threats are detected even when employees are working remote.

Incident Response

24/7 ASSISTANCE

Whenever your company faces a cyber incident, our Incident Response team is ready to help you to get back to business.

We are available day and night, even if you are currently not a client of Eye Security.

eye.

[COMING SOON]

Eye Cyber Insurance

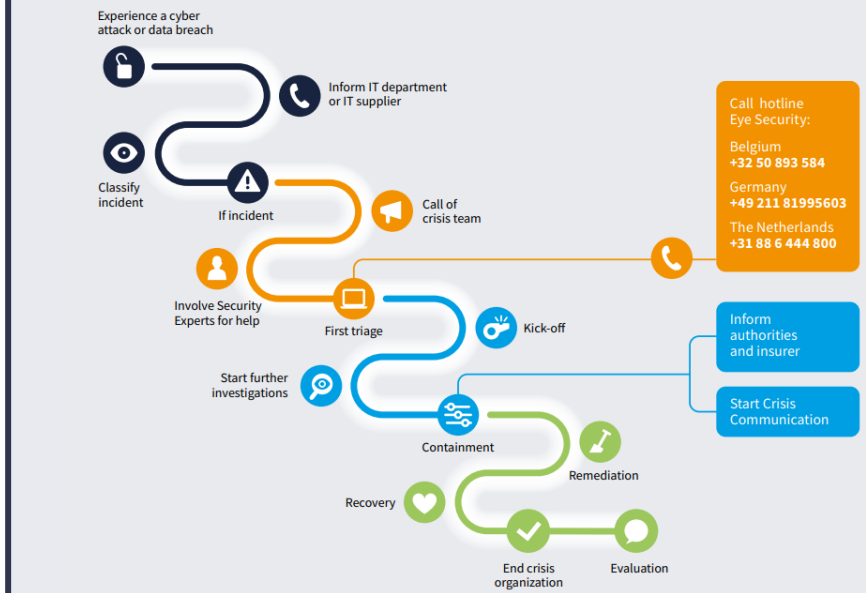
IMMEDIATELY INSURED

The financial damage caused by cyber-attacks can be devastating to your business. We take care of the financial damage to completely cover your cyber risk.

CONCLUSION

- Draw up, practice, and continuously improve on a good Incident Response Plan (IRP).
- Analyse your digital and online capabilities: weaknesses and strengths.
- Be aware of the consequences of a cyber incident (legal, financial, etc.).
- Strengthen your business by collaborating with a trustworthy cybersecurity partner.

Download Infographic:
How to act on a cyber incident



info@eyesecurity.be
www.eyesecurity.be
+32 50 893 584

Questions? Remarks?
Join the cyber discussion at booth 1005

THANKS TO OUR PARTNERS

nomeo

liantis

combell

Teamleader

eye cyber security

WORLDLINE

ESIGN

SIRIUS.LEGAL BUSINESS LAW FIRM

TRANS FORMA BXL

BUCKAROO

GET IN TOUCH WITH US

PATRICK MARCK
DIRECTOR

KERKSTRAAT 108, 9050 GENT
AV. J. BORDET 13, 1140 BRUSSELS

PHONE NUMBER
0475 33 08 71

EMAIL ADDRESS
PATRICK@FEWEB.BE