BDO RISK ADVISORY

AI DRIVEN PHISHING AWARENESS AS A SERVICE



TAILORED TO THE ORGANISATION AND ITS EMPLOYEES



Technological protection measures alone are not enough to protect your organisation against hackers. The most common cyber-attack is that hackers attempt to deceive your employees in order to obtain confidential information. Social Engineering (e.g. phishing and smishing) attacks are also becoming increasingly sophisticated and targeted.

While technology is continuously battling phishing, it does not adequately protect yourself against such attacks on its own. Continuously training your employees is therefore crucial so that they can recognise and respond appropriately to social engineering attacks.

It is important that the training is offered on a repetitive basis, so that your employees adopt the right reflex. In this context, BDO offers an automated AI-driven Phishing-awareness-as-a-Service program driven by the behaviour of the targeted employees and their responsiveness to phishing . By providing training tailored to the needs of the employee and raising awareness among them on a continuous basis, we ensure a significant improvement in your cyber security.

OUR APPROACH



Determining the Scope

Together with you, we will set the various

parameters and settings of the phishing AI.

Thereafter, the platform will be managed by

us to reduce the workload on your internal IT

department. The big difference in using AI to

raise your (cyber) self-defense, compared to

the traditional phishing campaign where one

email is sent towards all employees, is that

a wide range of different emails are sent out

to the employees based on their awareness

profile and their results on past simulations.

Furthermore, the emails are spread over

time in order to limit the risk of employees

spreading the word of an ongoing phishing

simulation.

2 Phishing simulations

Except for the whitelisting of our phishing platform, a simulation does not require the intervention of the Internal IT department. The AI will send out phishing emails to the employees based on their awareness level (and on the scope). Besides the manual import of a "target list" of employees using, an integration with the company's Active Directory is possible in order to keep the "target list" of employees up-to-date and optimize the use of your licenses.



Analysis & Reporting

These are non-aggressive phishing simulations, which means that we do not register any data (Password & Username) that may have been entered. Our simulations are fully focused on monitoring behaviour and its evolutions. In order to protect the anonymity of the employees, aggregated reporting is used. However, In depth reporting is available on the level of company, department, user, location, time & device type. Per user, information is available on their phishing awareness level, progression, the emails received, opened, phished ratio, data entry, etc. The use of detailed reporting will allow you to intervene where required.



S Repetition of the phishing cycle

At BDO, we believe that the creation of security awareness is a continuous process, not a one-off event. By implementing the automated AI-based phishing simulations, adapted to the ever-changing cyber world, we continue to measure and adjust security awareness. In this way, employees remain aware of the threats and are less inclined to respond to a real external attack.



4 Creation of security awareness

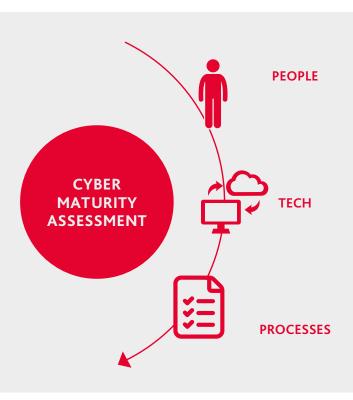
Following the simulations, employees are offered trainings that help them to better recognize such attacks and report them to IT. Depending on the awareness level of the user, defined by the AI, the user will receive additional awareness training initiatives targeted for their awareness level. Offered trainings will be short, in the language of the employee and to the point, the focus is on automating the correct response when confronted with a phishing attempt.



OUR CYBER SERVICES TAILORED TO YOUR NEEDS

Cyber security is a complex subject, in which many factors and measures come into play. Indeed, this is probably one of the reasons why so many organisations are reluctant to take decisive action. Unfortunately, there is no such thing as perfect security, which is why it is important to apply a risk-based approach, focusing first on the highest priorities and risk components. We will be happy to help you with that. As an independent third party, BDO advises organisations to take appropriate cyber measures. Since we do not carry out

any technical implementations ourselves, we are completely independent and our focus is on the most pragmatic solution tailored to the organisation. For each building block, we offer our customers a coordinated and technical approach with clear recommendations and concrete actions to ensure the confidentiality, integrity, availability and security of your data and systems. Our services are delivered by our certified and experienced professionals with the right, proven and effective tools for your entire organisation.



Simulation of a phishing attack **SOCIAL ENGINEERING** Physical security test **SECURITY AWARENESS** Live training on location TRAINING eLearning modules with optional exam **ACCESS MANAGEMENT** ✓ Logical access control review for applications and operating systems VULNERABILITY ASSESSMENT < Deep technical analysis of IT infrastructure **PENETRATION TESTING** An ethical hack to your organisation **POLICIES & PROCEDURES** ✓ Define and/or review the security policies and procedures **CONTROL FRAMEWORK** Prepare your organisation for control

Interested?

Get in touch with:

STEVEN CAUWENBERGHS

Partner Risk Advisory

E-mail: steven.cauwenberghs@bdo.be

Tel.: +32 497 05 12 23

FRANCIS OOSTVOGELS

Senior Manager Risk Advisory

E-mail: francis.oostvogels@bdo.be
Tel.: +32 474 92 08 00

ADVICE

NICK HUYSMANS

Manager Risk Advisory

E-mail: nick.huysmans@bdo.be Tel.: +32 486 31 90 45

frameworks (e.g. ISO27001, NIS Directive, CIS, ISF, etc.)



www.bdo.be

