Deloitte.

Stop phishing attacks

Tell me and I forget, teach me and I may remember, involve me and I learn.

The number of technical security measures within organizations is increasing over the past years. As a result, attackers are focusing more on the weakest link: the human factor. Phishing is a method where malicious e-mails are sent by cybercriminals with the intent to gain a first point of entry into the corporate network. Educating employees to recognize and respond to phishing attacks is the best step towards a more secure organization.

As computer systems become increasingly complex, the human component becomes an interesting entry point for attackers. Research shows that in 29% of successful data-leaks, employees provided access to attacker unintentionally [1].

Phishing is the practice where cyber criminals send e-mails to employees asking to perform a certain action. For example, clicking on a malicious link which installs software and allows an attacker to gain access to sensitive data or even take control over the system.

Training is often offered as a compliance exercise to educate employees about phishing. However, as employees move through the organization, new employees join the organization and over time, the awareness will fade over time, resulting in an ineffective training. Therefore, an effective approach should stimulate the employees to assess the emails they receive and reinforce the message over time.

We suggest a continuous phishing awareness campaign. With such campaign employees are trained and assessed with periodic phishing-attacks. These attacks can be executed in parallel with security workshops and e-learning modules.

Understanding the threat

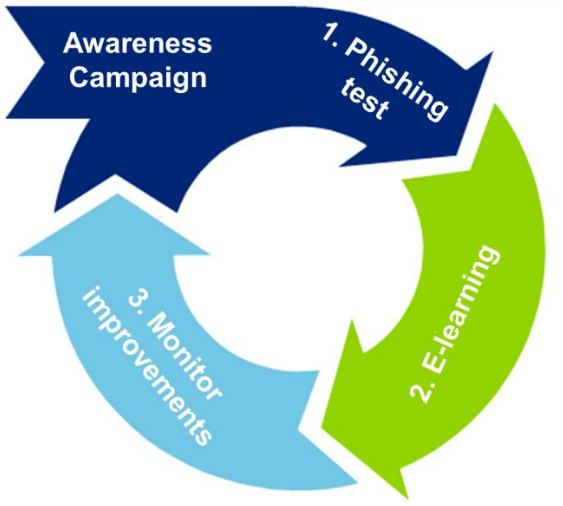
To protect an organisation against phishing, it is necessary that employees understand how cybercriminals work. A common attack vector is to forge the email address of the sender, for example, pretending to be a trusted colleague. Employees tend to fall for this trick as it is common human behaviour to help others in need. Attackers take advantage of such trust and human instincts.

How to respond

To quantify the risk of phishing within your organizations, it is necessary to measure employee behaviour in a privacy preserving and ethical manner. We provide the means to measure employee behaviour through customized phishing attacks as part of the ongoing learning cycle. The awareness is reinforced by a follow up e-learning module on phishing.

A combined solution

Our combined approach starts with an awareness campaign and is followed up with the following actions:



1. Testing the susceptibility of your employees.
2. Improving the phishing awareness.
3. Monitor the awareness improvement.

The awareness campaign starts with introducing the employee to the subject of phishing. During this introduction the employee will gain knowledge about phishing and the employee will be informed that at a given moment they will get first-hand experience with a phishing attack and an e-learning.

1) Source: Data Breach Investigations Report, 2013, Verizon, in cooperation with Deloitte.

Phishing test

Before the test stats, Deloitte supports the organization with the necessary preparation, such as how to deal with higher load on the IT-services, inform help desk to handle potential employee reactions and help in deciding the right phishing scenario.

When testing starts, Deloitte sends the crafted phishing e-mails to the (targeted) employees and measures a number of parameters, such as: how many employees click the malicious link, at what time were the links opened, what type of information the employees disclosed and the success rates among departments or business units. If the test is part of a recurring service, Deloitte can also provide trends between the tests, so the organization can determine the effectiveness of its awareness campaigns.

The infrastructure for executing the phishing tests is internal and assures the privacy of the shared information and the link between the employee and the results is preserved.

.

Awareness e-learning

After the test the employees can be informing about the results and what can be learned from these actions. As part of this feedback Deloitte also developed an e-learning including a final online exam. The training provides insight in the threats, educates the employees how to (re)act during an actual attack and improves the overall security awareness of the employee. Because the e-learning closely follows up on the phishing test, the employees are usually very interested in the material.

The e-learning can be customized for the organization, which ensures better transfer of knowledge.

The e-learning does not solely focus on the technical aspects, but also covers other areas such as psychology and business-impact. With a preliminary questionnaire, the content of the e-learning is dynamically adjusted to the level of knowledge of the employee. The e-learning can be provided in parallel with a workshops about general cybersecurity awareness, to raise the overall awareness and to answer questions about cybersecurity.

Monitoring awareness

The final step in the process is making the test results measurable. The phishing test results are anonymized and then presented to the employees. Per test we keep track of the results, by doing so the awareness level can be monitored. In addition the result can be used as input for consecutive phishing tests.

Deloitte offers a dashboard with statistics of the awareness level in regard to phishing within your organization. The statistics will not solely offer you insight into the progress within your own organization but will also allow you to see how your organizations is doing in comparison to organizations alike.

Why Deloitte

Deloitte has a broad range of experience when it comes to consultancy and assessment of information security within both private businesses and government institutions.

- Deloitte has plenty of experience with securely performing phishing attacks and reliably training organisations.
- Deloitte has an infrastructure to send thousands of e-mails per minute and store results securely and anonymously, in line with Dutch privacy law and legislations.
- Deloitte used the infrastructure, the training materials and the e-learning course for a number of clients. They are effective and can be easily tailored to provide a custom training, specific to the organization.

Also Forrester recognizes Deloitte as leader in their report “The Forrester Wave™: Information Security Consulting Services, Q1 2013. In compiling its ratings, the analyst firm cited Deloitte’s “exceptional client feedback and comprehensive, sophisticated, and mature service offerings.” The Forrester report also considered Deloitte as one of the leaders demonstrating deep technical expertise and global reach. Deloitte was the top-ranked security and risk consulting provider in the current offering category.

Contacts

Do you want to strengthen your organisation against phishing attacks? Please contact:

Trajce Dimkov
+31 6 1099 9115
tdimkov@deloitte.nl

Hugo Ideler
+31 6 8201 9188
hideler@deloitte.nl