TECHNICAL PHISHING TEST

Improve the entire chain of your technical e-mail defence

One of the most used initial attack vectors against enterprises is malicious mails sent to corporate email addresses. Innocent looking attachments or links clicked by unsuspecting users often lead to security incidents e.g., destructive ransomware attacks or stealthy information theft.

Value

- Increase your resilience to email-based attacks by letting Improsec help you locate any weak spots in your current e-mail defence, from the email security gateway to the user’s desktop.
- Get recommendations to your entire chain of the technical e-mail defence
- Prevent attackers from compromising your network

Product

The deliverable of the analysis is a written report containing the following:

- A non-technical section with an Executive Summary for management and decision makers

- A technical section including detailed observations and tangible recommendations to improve the security level and hardening of your e-mail defence

Method

Using our extensive experience from Red Team engagements, we create various payloads across different executable file types and send them through the email systems to the desktop. We observe if they are blocked or handled in a way that renders the attack useless, or if they are allowed to pass to and potentially be executed by the user. We test both payloads delivered as attachments and delivered via links. This is supplemented with specific test cases highlighting missing defence opportunities that we often encounter during engagements.

Based on this input, we analyse the level of sophistication required to bypass all defences and gain execution or access to credentials. Using this knowledge, we create examples of potentially successful attacks to showcase the value of finetuning the defence.

Invovlement

The delivery requires on-going involvement of your technical staff.

Improsec A/S
www.improsec.com
Telephone: (+45) 5337 5337
Email: info@improsec.com