terreActive

Success story

Preventing cyber attacks with audits and awareness training

terreActive audited and made the regional Bank SLM more aware of digital vulnerabilities

Attacks on websites and web applications, and the loss of confidential client data are threatening scenarios for any company. This is why Bank SLM had its web applications audited. In addition, it asked terreActive to prepare the bank's employees for various hazard scenarios using simulated attacks in the form of phishing.

A flashback to May 2017:
The regional Bank SLM from Münsingen (between Berne and Thun) faces two important milestones: An optimized website is launched together with a new partner. At the same time, a new web application for managing customer events is rolled out. Two changes that pose an imminent risk of cyber attacks.

Preventing rather than responding to attacks

Bank SLM sought help from terreActive. In addition to its security audit expertise, terreActive also provided its experience in the banking sector.

> *"The targeted phishing attack as part of the security awareness campaign was an educational experience for all of us.*
> *Thanks to this example of social engineering, we now know what an attack might look like, meaning that we are prepared for it."*
>
> Fabio Semadeni, Head of Services
>
> BANKSLM

The following goals were defined for the project:

- Identify vulnerabilities in the IT infrastructure, with a focus on the website and web applications.
- Raise the employees' awareness of cyber threats, with a focus on data theft through phishing e-mails.

Multi-stage approach

Technology – a weak point: Penetration test
The first part of the assignment, the audit of the website and the new web application, saw terreActive conduct an OWASP Top10 Standard audit by means of a manual penetration test. Using the targeted attack on the web application, vulnerabilities were detected in time and recommended measures could be implemented before a hacker could attack.

Humans – a weak point: Phishing
The employees of Bank SLM are already highly trained when it comes to handling sensitive client data. But the increasingly sophisticated methods employed by hackers make regular checks essential. A critical examination is also worthwhile at regular intervals with regard to organizational aspects such as processes and in-house interfaces. In this project, terreActive assessed the awareness by means of simulated phishing attacks.

Phishing is a form of social engineering that attempts to gain access to confidential information using fake e-mails.
The phishing attack at Bank SLM was carried out on particularly vulnerable groups of e-mail recipients. A subsequent malware infection would be another scenario.

This enabled employees to experience first-hand how attackers gain access to information. Awareness training organized by terreActive for the bank's staff following the project focused on the identified vulnerabilities and pitfalls.

Phishing remains a serious threat: Costs and potential damage to a company's image

E-mails with an unknown sender, suspicious subject or unusual attachment: Although phishing is nothing new, many companies are still affected and the damage caused is considerable. Coordinated attacks and preventive awareness training with employees prevent critical situations resulting in loss of revenue, infrastructure costs and image damage.

Why an audit is worthwhile

- The security infrastructure is examined by an independent body.
- Vulnerabilities to hacker attacks are identified and eliminated.
- An action plan helps with the implementation.
- The website is protected.
- The company is made more aware of potential phishing threats.
- Trained personnel raises security awareness.
- Sensitive data is better protected.

Tools used: LUCY – software made in Switzerland.

For this project, terreActive used the phishing software from LUCY, which puts IT security to the test by simulating realistic attacks. LUCY creates and sends e-mails, provides landing pages and training websites, and covers all reporting requirements. The terreActive audit team is a partner of the Swiss company LUCY Security.

BANKSLM

simply personally

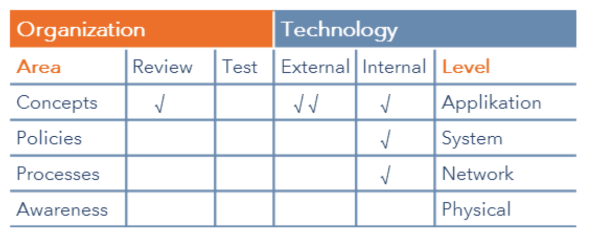
With more than 30,000 clients, around 70 employees and 5 branches, Bank SLM is firmly established in the region between Berne and Thun. It was founded in 1870 and serves both private and corporate clients.

www.bankslm.ch

Scope and content of the audit

At the beginning of an audit, it is determined which area should be examined and to what extent.

One possible example:



Organization			Technology		
Area	Review	Test	External	Internal	Level
Concepts	√		√ √	√	Applikation
Policies				√	System
Processes				√	Network
Awareness					Physical

We guarantee your success.
www.terreActive.ch