Phishing: effective protection starts with employees

terreActive strengthens cybersecurity at Kantonsspital Aarau with phishing simulation and awareness training

Phishing is one of the biggest gateways for cybercriminals. One wrong click on a fake email can have devastating consequences for a company. terreActive conducted a simulated attack at Kantonsspital Aarau to alert employees to the dangers with awareness training. As a result, the hospital is now prepared for possible attacks.

We've all seen them, because they pop up in our mailboxes almost every day – spam and phishing emails containing fake sender addresses, company websites or supposedly trustworthy requests to persuade users to disclose sensitive information or install malware. Senders of fraudulent messages usually give themselves away through spelling mistakes, non-specific forms of address or other inconsistencies. But phishing attacks are becoming more sophisticated and their success rate is increasing.

Personalized phishing messages addressed to individual recipients can pose a high risk for companies. They are often the gateway for hacker attacks that can have serious consequences, such as the installation of ransomware that encrypts data, directories or even entire hard drives and can only be decrypted by paying the hackers' requested ransom. This occurred in various cases where attackers succeeded in paralyzing parts of the IT infrastructure or even entire companies. Kantonsspital Aarau (KSA) was searching for a solution to better protect itself against such attacks. It found what it was looking for at the security specialist terreActive.

Putting security awareness to the test

KSA is the biggest hospital in the Canton of Aargau, with over 30 treatment and diagnostic centers, some 4,600 employees and capacity for over 28,000 inpatients.

"In the past, the issue of security awareness among employees wasn't addressed in detail. So tackling this problem was an important decision, and the right one, by the KSA security officers," said Martin Matter, CTO of KSA.

A package of various measures has proven to be effective against phishing attacks.

- It requires an anti-phishing strategy that the entire organization stands behind.
- The right tools are vital, including a solution capable of simulating attacks so an initial risk assessment can be prepared.
- In addition, awareness training is needed to keep all employees informed of the risks.

KSA turned to terreActive for support with these measures. With over two decades of experience in cybersecurity, terreActive was the perfect partner for this task and conducted a phishing simulation and awareness training. The first step of this process is a simulated phishing attack on the company is simulated to determine the current risk status and the existing level of employee awareness.

Tools in use:
LUCY Security made in Switzerland

The social engineering platform from LUCY Security offers a wide variety of features, phishing simulations, awareness training, reports and other services. The platform is upgraded regularly to keep pace with hackers' sophisticated methods. As an official LUCY partner, terreActive has many years of experience with the platform.
www.lucysecurity.com

Stages of the phishing project

The first stage of the phishing project was a kick-off meeting to define possible attack scenarios and awareness messages. After the technical preparations and final approval by KSA, terreActive's security experts sent a bogus email to KSA employees.
The phishing email was tailored to the hospital's circumstances, but also contained obvious mistakes, an unknown sender and other differences from messages usually sent to KSA. Despite all these red flags, a large number of employees contacted still clicked on the phishing link in the email. Many of them even entered their login credentials on the phishing website concealed behind the link.

"Our employees experienced first-hand the methods that potential attackers can use to obtain information," remarked Mr. Matter.

With its many years of social engineering experience, terreActive knows that KSA's results are within the norm, which unfortunately means that too many employees of other companies are also falling for bogus emails *before* receiving awareness training.

Forewarned is forearmed

After the email had been sent, the project entered its second stage – an awareness campaign. KSA employees were informed of the risks and best-practice conduct in the event that they receive suspicious emails or emails from unknown senders. A web-based course was also prepared for all the employees to determine their level of knowledge, address weaknesses and help them to detect attempts at phishing. terreActive assessed the results of both the phishing test and awareness training for the attention of KSA management and drew up a comprehensive final report containing statistics, an in-depth analysis, technical vulnerabilities and recommended measures.

Special thanks are due to all KSA employees who attended the training session in spring 2020, in the context of the extra stress of the first wave of COVID-19.

About Kantonsspital Aarau

Kantonsspital Aarau (KSA) is one of the largest regional hospitals in Switzerland, alongside the university hospitals. It provides services ranging from primary care to highly specialized medicine. It has vigorous research activities and a comprehensive range of advanced training courses for specialists.

In over 30 treatment and diagnostic centers, some 4,600 specialists working in diagnostics, medicine, care, treatment and other professional fields are responsible for almost 28,000 inpatient and over 520,000 outpatient treatments annually. www.ksa.ch

Kantonsspital Aarau

Emails from unknown senders, containing suspicious-looking subject lines or with unusual attachments – the problem of phishing might be well known, but companies are repeatedly affected and the damage inflicted is severe. Controlled attacks and preventive awareness training like the session held at KSA reduce the impact of an emergency in terms of loss of sales, costs of replacing IT infrastructure and reputational harm.

An effective anti-phishing strategy depends on employee awareness. While this knowledge is simple, the hurdles to creating this awareness are also great, despite the alarmingly high hit rate in the test. Many users are not interested in the issue, as CTO Martin Matter knows from discussions he's held with other hospitals. People are very unwilling to learn something new. Technical measures alone aren't enough to fend off attacks launched by cybercriminals. Well-coordinated teamwork between management, technology and employees is required – for example, through regular phishing simulations and awareness-raising measures, like those terreActive conducted for KSA.