REDGUARD
SECURING YOUR ASSETS

# SIMULATED CYBER ATTACK

**The KIBAG AG strives to protect its company assets daily. Those assets do not only exist physically, but increasingly in electronic form. Specifically designed cyber attacks for espionage and targeted malware are becoming an increasing threat. As a basis for improving and optimizing the existing system security measures, KIBAG has commissioned an attack simulation by Redguard.**

KIBAG. **Aus gutem Grund.**

KIBAG, established in 1926, is a leading Swiss group in the building and building materials industry. It is divided into three areas of business; building materials, building services, as well as environment and disposal, and has around 1600 empoyees. The KIBAG Group consists in total of 13 gravel and 22 concrete plants, 17 road and underground construction businesses, as well as several environmental- and waste management businesses. With their know-how, their integrity, and reliability they are at the forefront in the Swiss industry.

In 2016, KIBAG made use of Redguard's services and put its organization to the test through an attack simulation. To achieve this, specialists at Reguard carried out a realistic and risk-based attack on the whole organization. The goal was to identify technological and organizational weaknesses, to derive fitting measures and improve the security of KIBAG as a whole.


## KIBAG is attacked

KIBAG chose an external and independent service provider for the security audit of its information and communications technology (ICT) environment and business operations. Responsibility on KIBAG's side was assumed by the chief information officer (CIO), Christian Schollenberger. For him it was crucial that he was able to trust the Reduard team, and that they understood one another well. He was aware that Redguard would gain deep insight into KIBAG's systems and he knew that they would find some weak points. Christian Schollenberger: „I do not have any illusions, I know that our system is not perfectly safe." On the contrary, it was predominantly about being able to demonstrate to the management that the IT department has concerns about the ICT security and that there are possible risks.

As part of the attack simulation, the relevant worst case scenarios were defined together with Redguard. The specialists at Redguard have used these to develop tailor-made and realistic attack scenarios that were subsequently realized. Thus, for example, an attempt was made to infect the devices of KIBAG with a specific malware. The devices infected with the test malware then allowed further attacks on the internal ICT environment. The employees of KIBAG were also involved in the attack. The various scenarios of attacks reflect a real cyber attack on the company.

The results and corresponding suggestions for measures were summarized in the final report which was given to KIBAG as a basis for improving their security.

## Implementing measures as soon as possible

A list of internal measures was created on the basis of the results after the attack simulation. For Christian Schollenberger it was important that the measures were implemented immediately: „If you receive suggestions, they should also be implemented promptly – otherwise the whole thing is no good." An example of a possible cyber attack would be a Word document with a macro containing malware taking over a company notebook. This would allow an attacker to gain access to sensitive data. The sensitization of the employees is of immense importance here. The employees must be trained to recognize attacks and how to react in such a case in order to prevent further damage.

## Security is increasingly important

The CIO at KIBAG believes that it is very important to sensitize the employees accordingly: „A company not checking its system security is careless, because the ICT and information security is going to become even more important in the future, since we have a lot more network systems in our companies." Catastrophy is preprogrammed, if a hacker gets access to a system, because after the first attack other systems can be accessed, and finally the hacker will controll the whole ICT infrastructure.


**„Security is more and more important, therefore it is imperative that we have our organizations reviewed. An attack simulator is ideally suited for that."**

**Christian Schollenberger,** CIO

## A must for all companies

Auditing the ICT is not only called for in larger ventures, but in all organizations. „As soon as ICT systems and networks exist, security must be assessed", suggests Christian Schollenberger, „because ICT is the carotid artery of a company and when it is seized, it can have fatal consequences." The attack simulation lays the foundation for establishing organizational and technological measures to improve the overall security. The knowledge gained can also be used for sensitizing the management, as well as other employees. Thus all dimensions of security can be covered.

## Working with Redguard

Based on his positive experiences, Christian Schollenberger recommends working with Redguard: „The cooperation with Redguard was a complete success", says the CIO at KIBAG. Redguard was able to deliver essetial proposals for imporving security based on the conducted attack simulation. He is convinced that other companies will also be able to quickly build trust towards Redguard and their know-how. Schollenberger: „Redguard is absolutely trustworthy and competent. Your counterparts understand you and you receive a skilled answer to all your professional questions. The customers needs are respected and taken into account. That is the way cooperation makes sense and is fun."

Erstelldatum 04/2017, RG-C0