nixu
cybersecurity.

Cybersecurity exercises expose vulnerabilities in decision-making

Imagine you receive a call from the press: “Is your network under attack?” they ask. What will you say?

WHITEPAPER

WHITEPAPER

We prepare for fires: We are given advance warning about a fire drill, and when the fire alarm goes off, everyone exits the building. We all know the signs for emergency exits and the location of assembly points where we are expected to gather. But how does your organization react in the event of a cybersecurity incident? Who does what? Like fires, cybersecurity incidents are something we can prepare for.

Contents

Introduction

The company's network is down, production is managed manually, Twitter updates are conspicuous by their absence… who should you notify first? How quickly must you act? And where are those instructions? All too often, we are left trying to remember who is responsible for what when a data breach, denial-of-service attack or another cyber threat is upon us and there is no time to waste.

To make sure that in a real cyber emergency no panic ensues, cyber events should be prepared for with exercises. Cyber exercises of varying extent can be carried out in all kinds of companies. At their shortest, they may constitute a session lasting a couple of hours, while at their most extensive, an exercise may be spread over several days and take place in a number of locations.

In this article, I will describe what a cybersecurity exercise entails in practice, the steps it involves, and the surprises that typically emerge in the course of it. I will also explain what our customers think about the exercises. And to conclude, I will dispel a few myths related cyber exercises.

Rehearsals for all needs and purposes

There is a wide range of cyber exercises designed to meet various needs. At its most basic, an exercise may refer to the annual revision of correct measures in the event of a payment card-related incident required by the Payment Card Industry Data Security Standard (PCI DSS) audit. At the other end of the spectrum are rehearsals that cover the organization's entire cybersecurity system over the course of multidimensional live training sessions.

Participants in the exercise

At a minimum, the training is attended by a helpdesk representative, a representative of the external service provider and, when necessary, the employee responsible for notifications to authorities. Participants in the more extensive rehearsals typically include employees from product development and other similar functions as wells as managers. Other important participants include units that are not directly involved in cyber operations, such as communications and HR.

The consultants are represented by a game leader, tasked with time management and other arrangements. To avoid the need for the customer's representatives to be present throughout the training, Nixu's consultants can represent these virtual persons. Two or three consultants are on hand to answer any questions during the exercises. In addition, one or two observers are present at the training to analyze how the participants act, organize themselves and make decisions.

In total, 9 to 14 people take part in the exercises, including 4 to 7 people from the customer's organization and 5 to 7 consultants from Nixu.

Duration of the exercise

Preparations for the training take 4 to 8 calendar weeks. Our cybersecurity consultants plan the scenarios to be played out during the training on the basis of relevance. They must include several alternatives to accommodate the choices made by the participants and the events that arise as a result.

At the planning stage, the customer provides information on its environment and technical solutions. The customer's contribution to this stage is critical in order to create a realistic scenario that could emerge in the organization in question. We recommend allocating a few workshop days for these tasks at various levels of the organization (technical and administrative). The consultant responsible for the preparations interviews members of the staff with regard to their areas of responsibility.

On rehearsal days, either the morning or afternoon should be set aside for the training. In the case of a more extensive exercises, the training may last longer than a typical workday (for example from 8 am until 6 pm) or it can take a couple of normal workdays.

The exercises are always planned to meet the customer's specific needs and there is no one-size-fits-all solution. Often, our exercises kick off with a long-term e-mail campaign and culminate in an on-site training day. Also, international training events with participants coming from various market areas can be arranged. When it comes to cyber exercises, the sky's the limit.

Purpose of the exercises

The most common scenario prepared for in cyber exercises involves a personal data leak because such an event always requires collaboration with authorities and certain legal requirements are imposed on the process. The data breach may also concern the company's product information, in which case the GDPR process is not applied. Furthermore, another scenario that is often covered involves cyberattacks that may pose a financial threat. As there are numerous types of cybersecurity risks that businesses can face, potential training scenarios are abundant as well.

What cyber exercises entail

Preliminary work

All the exercises are based on the customer's needs. Imaginary training scenarios that are based on our consultants' guesses about the customer's processes would not bring the desired results and that's why we always build the exercises around the processes in place in the company.

When a company makes a decision on a cyber exercise, the first step involves gathering background information. During this stage, our cybersecurity consultants learn about your organization and carry out background research. After that, we can agree on the schedule and participants.

Upon request, we can also develop a scenario for which the customer has no readymade process in place. This allows you to see how your employees organize themselves and how the decision-making process is formed.

Training day

Cyber exercises are carried out as tabletop exercises. In practice, this training format involves key personnel gathering in a meeting room to discuss a simulated emergency situation. Focused on decision-making processes, the training does not require actions on a technical level and our consultants do not interfere with production systems.

The exercise kicks off with the game leader providing initial information on the incident. This may involve a data leak in a partner's system, trojan malware or a clever phishing scheme. Perhaps a disgruntled employee has tinkered with the company's code and is now trying to sell data over an anonymous network? The scenario can be anything that is relevant to the company.

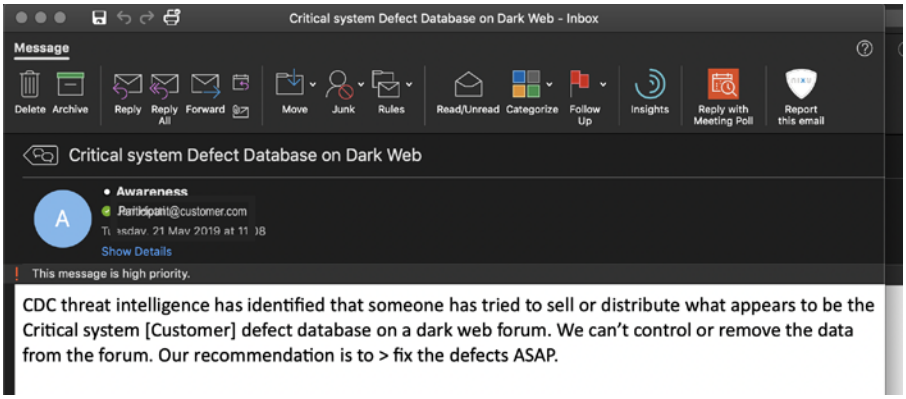
A journalist from a local tabloid calls the IT manager and says: "We hear you have a situation there." How do you respond?

The participants are given some time to take in the initial information and to discuss it. What are the consequences of the event? Are they interested in it? Should they be interested?

After a while, the discussion is stopped and the situation is processed with the game leader. Do the participants see the situation in the same way as the game leader?

At the next stage, the participants have to organize themselves in line with the requirements of the scenario. They are given evidence that confirms that the emergency is real. Then the participants take measures in compliance with the company's procedure. The game leader pauses the training at set intervals to give the participants the opportunity to reflect on their actions.

As the game progresses, the participants are given input via an electronic platform or playing cards designed for the purpose. While the electronic platform speeds up the progress, all the exercises are easy to carry out as tabletop activities without the need for any technical devices.



During the exercise the game lead provides the participants with new injections. The injections can be e.g. emails.

Your service provider informs you that the number of hits against the firewall is high. What do you do?

After providing the original information, the game leader may not intervene in the progress of the exercise, particularly if the training is a exercise related to a PCI DSS audit, in which case the participants know the process well. However, often the game leader likes to throw a curveball. This may involve providing misinformation that throws a spanner in the works.

The customer service has received several notifications about problems with payment transactions. What do you do?

One way of adding difficulty to the exercise is to carry it out as a deputy training, in which case all the participants are not the persons in charge of the matter but their deputies who have not received as much training. In this case, the participants typically have to rack their brains a little to remember where to find the relevant instructions and who to contact. The game leader may increase the pressure by hurrying the participants or by providing information that is not relevant to the task at hand.

If the participant does not have any idea about the correct procedure, the game leader may offer a hint, along the lines of "You might want to call someone." Usually, no alternatives to choose from are given unless the participant fails to respond to the input from the game leader.

As described, the simulation exercises involve alternating periods of practice and reflection. The game leader offers input and prompts the participants, virtual persons answer questions and observers monitor the situation. The participants must give it their best effort.

The injection could be imaginary print screens to which the participants need to react.

Feedback and measures

I've never encountered a customer who didn't know the steps to take. Professionals know what they are doing. While not everyone may know the procedure, one member of the team typically steps up and leads. Sometimes I have to offer more guidance, while at other times I end up adding difficulty to the exercise by springing surprises on the participants.

Customers really enjoy cyber exercises. They find that the twists and turns that take place in the course of the exercise stick in their minds and new skills learned this way are easier to apply than information garnered from a long report. Usually, concrete measures materialize as a result of the rehearsal. It is not rare for the companies to launch development projects and to improve their processes and guidelines after training.

We have the capacity to determine all the possible risks and we are regularly praised for our expertise. A cyber exercise offers the opportunity to practice life-like situations where data is under threat.

Four myths about cyber exercises

I often find myself defending the need for cyber exercises in various contexts. People often entertain erroneous assumptions about the topic. Let's look at some facts.

1 "I doubt anyone would be interested in our company's data, so for us, cyber incident simulation exercises are a waste of time."

These days, it's hard to think of an organization that is not affected by cyber risks. (Let me know if you can think of one!) If your organization processes information via the internet and carries out operations online, a cyber attack is a realistic threat.

If you look at your process diagram, you are likely to notice that you don't just manage your own data and money but also those belonging to your subcontractors, customers and partners. With today's networked business operations, even if you don't think your company's data is worth protecting, you surely want to nurture your business relationships.

What will you say to your partners whose data has been accessed and destroyed though your system by a hacker? You should rehearse your answer.

2 "Cybersecurity exercises are expensive and time-consuming."

A single stolen record (such as a password) costs a company about 148 dollars on average. About 65% of British customers who were affected by a data leak lost their trust in the company and 27% ended their customer relationship, while 11% became targets of one or more cyber crimes. A company with a low level of information security lost about a million pounds more of their turnover as a result of a data breach than companies with a high standard of information security. Companies with low information security standards typically see their share prices drop by more after a data breach than companies with higher information security standards.

With everyone knowing the high cost of fires, you don't really hear people bemoan the cost of fire drills. Cybersecurity exercises typically cost a fraction of the potential losses caused by a data breach.

3 "Because of GDPR, we already have an information security plan in place, so we don't need cyber exercises."

Pursuant to legislation, companies must implement appropriate personal data practices so it's good that your company complies with legal requirements. But unfortunately, cyber criminals are interested not only in personal data but also in product information. The main motive for attacks is financial gain. What are the financial losses and production delays that your company is prepared to suffer as a result of having to test run your cyber attack procedures in a real emergency?

4 "The information security consultants just nitpick about minor issues that are of no real consequence."

The feedback from a cyber exercises always compares observations with the best practices. The report examines the exercises in the context of pre-determined expectations, observations and proposals for improvement. The final report offers a tool for further development.

What's more, a cybersecurity exercises in itself is a concrete measure that can enhance the company's standard of cybersecurity. I wouldn't call these minor issues!

[1] Ponemon Global Cost of a Data Breach Report 2018
[2] Ponemon Data Breach Impact Study UK 2017

Written by

Anu Laitila,
Cybersecurity Awareness Business Manager

nixu cybersecurity.

Contact

/nixuoy
@nixutigerteam
/company/nixu-oy

nixu.sales@nixu.com
www.nixu.com

Nixu is a cybersecurity services company on a mission to keep the digital society running. Our passion is to help organizations embrace digitalization securely. Partnering with our clients we provide practical solutions for ensuring business continuity, an easy access to digital services and data protection. We aim to provide the best workplace to our team of nearly 400 cybersecurity professionals with a hands-on attitude. With Nordic roots we serve enterprise clients worldwide. Nixu shares are listed on the Nasdaq Helsinki stock exchange.