Ransomware: what measures can be taken to counter the threat?

Ransomware has become the bane of IT departments and businesses in general. But is it inevitable? We asked Sébastien Viou, Stormshield's Director of Product Cybersecurity and Cyber-Evangelist, what steps are needed to address this issue.

01

PROTECT YOURSELF BEFORE THE ATTACK

BACK UP DATA... AND PROTECT BACKUPS

"This precaution alone is not enough, as this is the first thing that the ransomware will seek to destroy, even before encrypting. It is necessary to use off-line tape backups and to correctly work out the frequency of these backups. It is also necessary to test restoration mechanisms to ensure that the backups are usable.".

KEEP SOFTWARE AND SYSTEMS UP-TO-DATE

"Updates should be applied continuously, and include not only Windows PCs but also Linux and Mac systems, which can also be entry points. The entire office environment is affected, from Microsoft Exchange to Active Directory and all exposed servers, even small ones.".

PARTITION THE INFORMATION SYSTEM

"The recommendation for doing this is to apply strict rules regarding permitted data flows between different areas, based on their criticality."

LIMIT USER RIGHTS AND APPLICATION PERMISSIONS

"In this respect, the decisive factor is management over time: to maintain safety, regular reviews must be planned."

IMPLEMENT A LOG SUPERVISION MECHANISM

"Log collection is a must. In cases where a very high level of security is required, it is possible to add an intrusion detection component via an SOC."

RAISE EMPLOYEE AWARENESS

"With social engineering, the main gateway to a company's information system continues to be its employees. It is therefore important to talk about cybersecurity issues, despite the fact that awareness-raising has its limits."

PLAN OUT YOUR CYBER CRISIS COMMUNICATION STRATEGY

"In this case, too, it is useful to have planned your messages and contacts beforehand in order to communicate appropriately with the different audiences. Communications used to warn of unexpected production stoppages, for example, or leaks of personal data, as required by the GDPR."

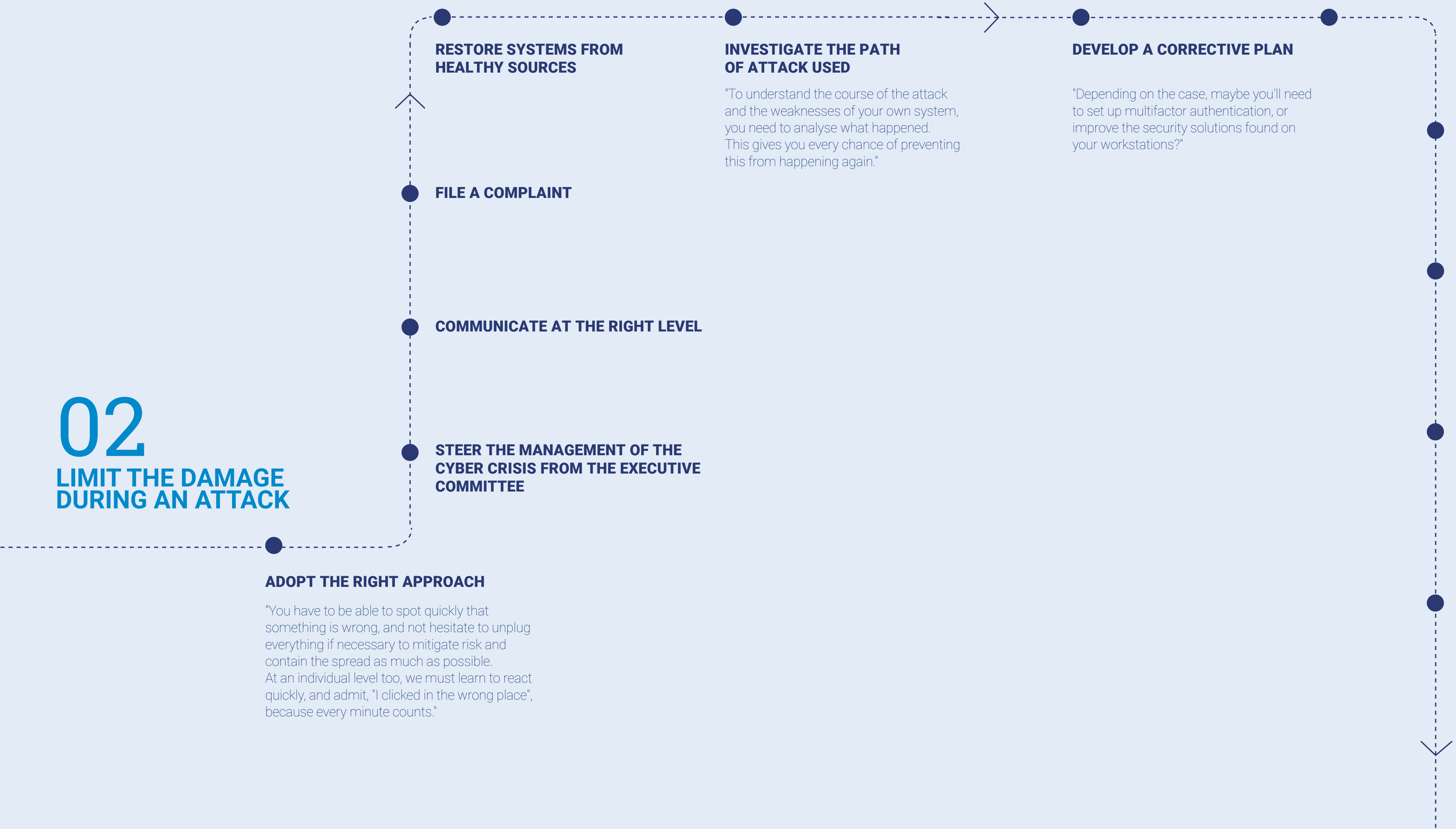
IMPLEMENT A CYBERATTACK RESPONSE PLAN

"This plan is crucial, as it makes it possible to react quickly; for example, by contacting pre-identified CERT companies. It obviously includes a technical component, with the implementation of protection solutions such as Stormshield Endpoint Security Evolution and Stormshield Network Security."

ASSESS THE BENEFIT OF BUYING CYBER-INSURANCE

"Some cyber-insurance policies include clauses on the deployment of cybersecurity solutions; they are worthwhile in that they force companies to adopt certain protection measures. However, cyber-insurance should not be seen as a survival measure on its own, and even less as a protection measure. In other words, insurance against ransomware will never constitute a cybersecurity strategy."

STORMSHIELD



02

LIMIT THE DAMAGE DURING AN ATTACK

ADOPT THE RIGHT APPROACH

"You have to be able to spot quickly that something is wrong, and not hesitate to unplug everything if necessary to mitigate risk and contain the spread as much as possible.
At an individual level too, we must learn to react quickly, and admit, "I clicked in the wrong place", because every minute counts."

STEER THE MANAGEMENT OF THE CYBER CRISIS FROM THE EXECUTIVE COMMITTEE

COMMUNICATE AT THE RIGHT LEVEL

FILE A COMPLAINT

03

RECOVER AFTER AN ATTACK

RESTORE SYSTEMS FROM HEALTHY SOURCES

INVESTIGATE THE PATH OF ATTACK USED

"To understand the course of the attack and the weaknesses of your own system, you need to analyse what happened.
This gives you every chance of preventing this from happening again."

DEVELOP A CORRECTIVE PLAN

"Depending on the case, maybe you'll need to set up multifactor authentication, or improve the security solutions found on your workstations?"

ESTABLISH A PRODUCTION PLAN TO CATCH UP ON LOST TIME

TAKE LEGAL ACTION, IF THIS HAS NOT ALREADY BEEN INITIATED

MANAGE THE PSYCHOLOGICAL IMPACT ON EMPLOYEES

"Ransomware also has consequences for human resources – including short-time working, guilt and overworked IT teams – which need to be taken into account."

ROLL OUT THE COMMUNICATION PLAN TO IMPACTED CUSTOMERS, YOUR INVESTORS, ETC.

SUBMIT THE CLAIM TO THE INSURANCE COMPANY