Article

Interview with Erik Sennfält,
Senior Country Manager at Sectra

Secure communication — Technology only half of the picture

Cyberthreats are here to stay, with attacks becoming increasingly common and sophisticated. Secure communication requires a combination of effective technical solutions and an understanding among users of the importance of acting in a secure manner.

Developments in cybersecurity and secure communication are moving quickly. The Swedish Security Service, the National Defence Radio Establishment and the Swedish Military Intelligence and Security Service have noted a growing activity rate and more serious threat level in Sweden for many years now—with threats originating from foreign powers and criminals, and even from unholy alliances between the two.

"This affects the entire spectrum, from the media and politics to industrial espionage and stealing military secrets," says Erik Sennfält, Senior Country Manager at Sectra.

What is a cyberthreat?

A cyberthreat is a collective name for activities aimed at stealing, distorting or otherwise influencing information, most commonly using the internet as a means to do so.

From a technical standpoint, it's a cat-and-mouse game between security solutions and attackers. Measures are taken to fix new security loopholes that criminals discover and abuse. But technology is only half of the picture when it comes to cybersecurity.

"The weakest link in the chain is people. Many breaches are the result of human error—being careless about authorizations, weak passwords, lost passwords or clicking on a corrupt link."

Attacks becoming increasingly sophisticated

Corrupt links are often found in phishing emails. These may appear to be genuine messages in terms of the language and graphics used. They may appear to originate from your bank, a supplier or your manager.

"The best protection against this threat is regular micro training, such as reminders and status updates to keep employees aware of the risks."

Micro training can be used, for example, to provide information about what to do when opening links, emails or shared documents and how to recognize when something is not genuine.

“Something that everyone needs to understand is that what is considered secure today will definitely not be in the future. Assessing security classifications for various kinds of data is a fundamental aspect of data-security work, and something that Sectra has considerable experience of.

“The question you need to ask yourself is what would happen if the wrong people were to access sensitive data and compromise it? Or if they were to prevent you from accessing it? What would the consequences be? For individuals, the organization and the country as a whole.”

The right level of security

For a company, sensitive information may include price lists or blueprints. For a public authority, however, it may include registers or maintaining round-the-clock services. All of this determines how, where and with whom data should be stored in order to ensure compliance with applicable legislation and maintain the right level of security.

“One example of processes that are difficult to assess is software build processes—who has done what and when. There have been cases where malicious entities have compromised well-established software developers and manipulated products to spread malicious software.”

Erik Sennfält explains that there are plenty of security solutions available and underscores the importance of choosing a solution from a reliable provider. Among other solutions, Sectra offers a VPN that provides intrusion protection and ensures that only the right people have access to the information. Another example is Sectra Wire, an end-to-end encrypted solution for digital collaboration that protects users against eavesdropping in their daily communication via chat or video conferences.

“The most important thing is that the security solution is transparent for the end user. The user shouldn’t need to think about the solution being in place.”

If a higher level of security is required, such as two-factor authentication, the user needs to accept this.

“If staff understand why certain procedures need to be followed, this minimizes the risk of shortcuts being taken and compromises being made. In this way, Sectra acts a partner to help organizations implement and maintain the right level of security.”

“The question you need to ask yourself is what would happen if the wrong people were to access sensitive data and compromise it? Or if they were to prevent you from accessing it? What would the consequences be? For individuals, the organization and the country as a whole.”

Sectra Communications AB • communications@sectra.com • communications.sectra.com

SECTRA
Knowledge and passion