Protection against cyberattacks requires smarter approach

March 10 2022

Credit: Pixabay/CC0 Public Domain

If companies want to more efficiently limit the risks of cyberattacks, they should invest smarter rather than more. Many organizations currently still mainly select their investments based on past information, but choosing a flexible approach based on system dynamics would provide ample space for improvement. This is the point made by Sander

Zeijlemaker, who will obtain his Ph.D. from Radboud University on 16 March.

Stories about large organizations being targeted by ransomware, malware and other cybercrime reach the news almost daily. These attacks lead to significant expenses, but also to leaked private data and, in extreme cases, even to highly classified information being exposed. It is a world in which the attackers and their approach continuously evolve and innovate. However, while companies grow or shrink and continuously deal with new situations, their security policies only get limited adjustments.

Zeijlemaker: "Managers who have to make decisions regarding cybersecurity are supported by various standards, frameworks and comparisons to other organizations. After every incident, whether internal or at another company, new measures are taken to prevent another incident. However, this approach is rather static; it could be compared to driving while only looking in the rear-view mirror. People often like to think they are very adept at making decisions and assessing situations, but it can be extremely difficult for a single person to consider and see all consequences of a choice."

System dynamics

In his research, Zeijlemaker considered an approach based on system dynamics. This approach has been in use for quite some time in various other areas, ranging from medical research to sustainability. "However, it is still barely used in the field of cybersecurity," Zeijlemaker says. "In this approach, you start by identifying all factors, including their interconnectedness, that should be taken into consideration when taking strategic decisions regarding cybersecurity. These factors include the development of the attacker, the behavior of staff and the quality of the measures taken. This information and the relevant data are then used to

create computer-aided simulation models."

"The main benefit of this approach is that it can imitate decision-making processes and provides insight into the future effects and consequences of strategic choices. The advantage of simulations is that they can show a multitude of possible choices without those having direct consequences on the company operations, as opposed to reality, in which decisions do have direct consequences. We can make an adjustment to a single variable and see what the expected effect is on the other variables." The world of cybersecurity is dynamic, and the strategic approach should be as well.

Preventing high expenses after the fact

Zeijlemaker warns that companies will have to actively mind their cyber policy. "Its not just an expense that should be increased or decreased carelessly. Companies should start internal discussions: what are we spending our money on, and why are we doing that? By making use of this kind of models, we can take a much more future-oriented approach and make proactive decisions. This is crucial, as too many companies are still insufficiently prepared. They assume that, if need be, they can put some money aside to fix the situation after the fact, but that often turns out to be much more expensive than they are counting on. Furthermore, private data and other sensitive data will often have leaked out by that time. By monitoring the situation proactively, they can prevent additional costs and problems."

Provided by Radboud University