Horizon
The EU Research & Innovation Magazine

European Commission

Researchers and small businesses join forces against hackers

Improved cybersecurity defences for electronic commerce have emerged from EU-funded projects.

22 February 2024 - By TOM CASSAUWERS

What do a Greek pharmacy, a Spanish multinational bank, a German foundation specialised in the digital economy and a UK university have in common?

They all helped develop software tools with EU funding to counter cyber and physical threats to e-commerce in the European single market, the world's most lucrative.

Prime targets

Called ENSURESEC, the project sought to ensure that small and medium-sized enterprises, or SMEs, in particular have adequate technological knowledge and defences against hackers and fraudsters.

'SMEs have fewer resources,' said Luis Carrascal, a cybersecurity expert at French software company Inetum. 'They can't just hire large teams of cybersecurity experts. The majority of SME employees also lack a basic understanding of cybersecurity.'

SMEs are defined as businesses that employ fewer than 250 people and have annual turnover of no more than €50 million. They account for almost all companies in Europe, making them regular targets of cyber-attacks.

Nearly a third of European SMEs faced at least one cybercrime in 2021, according to a Eurobarometer survey.

A typical example involves a "ransomware" attack in which hackers enter a company's computer systems, encrypt their data and demand a ransom. A European network of small businesses reported a 57% increase in ransomware attacks on SMEs in 2023 compared with the previous year.

'Attack surface'

Theodoros Sakopoulos, who owns an online pharmacy called ToFarmakeioMou in the Greek capital Athens, simulated a hybrid physical and digital attack during ENSURESEC.

In the mock theft, hackers tried to jam the GPS tracker of a drug delivery by the business so they could intercept the truck and steal its contents. Sensor devices were developed to track the shipment and notify the pharmacy when any order got tampered with.

Sakopoulos was among 22 participants in ENSURESEC, which ran for two years until mid-2022. Other participants included Spain-based CaixaBank, the IOTA Stiftung – a German foundation advancing research into the digital economy – and the University of Greenwich in the UK.

'The attack surface is huge in e-commerce,' said Augustin Lemesle, a research engineer at the French Alternative Energies and Atomic Energy Commission, or CEA, which also took part in the project. 'You can be attacked from everywhere.'

Lemesle was the technical coordinator of ENSURESEC, whose participants came from 14 European countries. Other participants included the Spanish office of French software company Atos and Belgian university KU Leuven.

AI vigilance

One of the project's software tools uses artificial intelligence (AI) to monitor a company's internal networks, which are shielded from the outside internet. They're the grand prize for hackers, who seek entry to gain access to sensitive data.

That's why monitoring such internal networks for suspicious activity is key for keeping a company safe.

Doing that manually is hard because of the high number of people using these networks and because of their complexity. By contrast, an AI system can do this automatically 24 hours a day and report anything out of the ordinary.

'We need to ensure that a company reacts well when a threat appears,' said Lemesle.

Online buying has boomed since the Covid-19 pandemic erupted in 2020.

The turnover of European e-commerce increased by 6% to €899 billion in 2023 compared with the previous year. Growing numbers of SMEs are serving their customers through the internet, which makes them a bigger target for attacks.

'E-commerce is very closely linked to consumers,' said Lemesle. 'If something goes wrong there, it has a very big impact on society. Everyone is using e-commerce, which puts our personal data and security at risk.'

Easy-to-use kit

Inetum's Carrascal led a separate EU-funded research project to develop cybersecurity defences that are easier for smaller European businesses to use.

Called CyberKit4SME, the project ended in November 2023 after three and a half years.

Carrascal said the difficulty for smaller businesses isn't an insufficient number of software options to address cybersecurity but rather their complexity.

'There are already a lot of software tools on the market,' he said. 'The issue is that they're complicated to operate. That's a problem for SMEs, which don't have big IT teams.'

One of the software options from the project helps SMEs store and access their data more securely.

A second looks at how people behave on the company's networks and where dangers may lie.

The human dimension is the weakest link in a company's cybersecurity setup. People might, for example, click on an infected link, giving hackers access to the company's internal networks.

Yet another piece of software from the project seeks to spot security vulnerabilities through the modelling of IT systems.

‘It allows companies to create a virtual model of their information system, which helps them analyse possible threats,’ said Carrascal.

At present, this kind of software requires an information-technology expert to go through a company’s software system and list all the places where it can be accessed from the public internet. This creates a list of possible hacking entry points that in turn need to be protected.

By automating more of this process, CyberKit4SME has made it easier for smaller companies to improve the security of their computer systems.

Market tests

Both CyberKit4SME and ENSURESEC are keen for their technologies to enter the marketplace.

ENSURESEC has grounds for optimism.

Some companies are already selling tools developed during the project, while other tools have been made open-source, according to Lemesle.

‘There’s real demand for our technology,’ he said.

Other technologies that emerged in ENSURESEC need further development, some of which is being done in new EU-funded research projects, according to Lemesle.

CyberKit4SME too has been disseminating some its software for free.

Of six technologies developed in the project, four have been made fully open-source and one partly, according to Carrascal.

‘Anyone can use them,’ he said.

Furthermore, some project partners are considering creating a startup business to commercialise the whole toolkit, according to Carrascal.

‘Attackers will keep exploiting less prepared organisations,’ he said. ‘That’s why we need to invest in better protecting them.’

Research in this article was funded by the EU’s Horizon Programme. The views of the interviewees don’t necessarily reflect those of the European Commission. If you liked this article, please consider sharing it on social media.

More info

- ENSURESEC
- CyberKit4SME