Horizon
The EU Research & Innovation Magazine

European Commission

European cybersecurity is getting its own legs to stand on

With cyberattacks on the rise against everything from businesses to critical infrastructure, companies, governments and researchers are joining forces to strengthen firewalls.

08 February 2023 - By TOM CASSAUWERS

In February last year, as oil prices spiked following Russia's invasion of Ukraine, computers stopped working at the Amsterdam-Rotterdam-Antwerp oil trading hub. This group of terminals concentrated at some of Europe's biggest ports had fallen victim to a cyberattack. Barges couldn't be unloaded and supply was disrupted.

Cyberattacks on critical infrastructure like energy companies, hospitals and government agencies have become common occurrences. The European cybersecurity agency, ENISA, encountered 623 ransomware incidents from May 2021 to June 2022. Each month, 10 terabytes of often-confidential data were stolen in this way.

Homegrown need

'In the past years we have seen an exponential increase in the amount of cyberattacks and the damage they cause,' said Matteo Merialdo of RHEA Group, a Belgian cybersecurity company that is a project manager in the EU-funded ECHO project. 'We need a European response.'

Europe is heavily dependent on US software providers for its cybersecurity and building more European alternatives could make the continent better able to fend off attacks, according to Merialdo, who is RHEA's deputy business unit manager of security services and has a Master's degree in software engineering.

Europe is trying to strengthen its homegrown cybersecurity industry, with researchers and companies developing new tools and building up so-called strategic autonomy amid heightened geopolitical rivalries worldwide.

In a sign of how cybersecurity has jumped up the European political agenda, the EU in 2020 imposed cyber sanctions for the first time by blacklisting a number of Russian, Chinese and North Korean hackers.

‘We of course needs allies like the US,’ said Merialdo. ‘But American companies are making a lot of money in Europe, which could go to European companies. At the same time, we need to be able to stand our ground with local solutions in case we come under attack.’

Just why this is important was signaled when Russia launched its full-scale military assault against Ukraine on 24 February 2022. Russian cyberattacks repeatedly targeted the country and its infrastructure before and after the invasion.

‘The ways to wage war are changing,’ said Merialdo. ‘War doesn't just extend to the sea, air and land anymore, but also to cyberspace.’

Microsoft’s Digital Defence Report 2022 recorded 237 cyber operations targeting Ukraine in the six weeks leading up to the invasion. Attacks have also continued since then.

‘Launching cyberattacks is cheaper than buying fighter jets,’ said Merialdo. ‘Yet they can still do quite a lot of damage.’

Testing ground

ECHO, which ends this month after four years, has brought together a number of European cybersecurity players to develop software that could prepare for and mitigate cyberattacks. The project is coordinated by Belgium's Royal Military Academy. Merialdo, who also has a degree in telecommunications engineering, stressed the goal of strengthening the capacity within Europe to deal with these challenges.

‘There's a huge technological gap with the US – there's not a knowledge gap,’ he said. ‘Europe has very strong research and in-depth knowledge. But we use too many US tools. We have to mitigate this gap because it threatens our sovereignty.’

Among other research the ECHO team focused their attention on Cyber Range technologies. Cyber ranges are testing grounds of sorts in which organisations can put their cyber defences under pressure without compromising their actual systems.

Cyber ranges allows its users to construct a detailed reproduction of their digital systems. This copy can then serve as a training ground for employees. All kinds of attacks can be thrown at them, without disrupting their actual work, according to Merialdo.

‘It's an emulation of reality,’ he said. ‘A nuclear power plant can, for example, organise an almost real exercise. If a space control centre wants to test its operators on how to respond to a cyberattack, you cannot do that on the main network. If you do, you risk knocking your satellites out of orbit.’

Cyber ranges come in many shapes and sizes. National defence agencies often employ expansive cyber ranges to simulate large-scale cyberwarfare.

But tools like the one developed by ECHO can also just be employed by individual companies to train their cybersecurity staff. According to Merialdo, developing this sort of technology inside Europe is an important step for the region's strategic independence.

Because of increasing digitialsation, even places like space control centres are vulnerable to cyber-attacks. Everything from household appliances to basic government services rely on digital connections and, as a result, need someone to protect them from attacks.

‘Cybersecurity is now everywhere,’ said Merialdo. ‘It's in hospitals, space missions, nuclear power plants or even just our houses.’

More teamwork

ECHO helped lay the groundwork for the creation in 2021 of the European Cybersecurity Competence Centre (ECCC). Located in Romania, the ECCC coordinates European cybersecurity projects, funds them and aligns the work of national cybersecurity agencies.

‘A lot of funding goes into cybersecurity,’ said Nick Ferguson, a senior project manager at Italy-based marketing and research business Trust-IT Services. ‘But before there wasn't always a lot of coordination between companies, projects and researchers.’

He led the EU-funded cyberwatching.eu initiative, which ended in mid-2021 after four years. It developed an interactive overview of all EU-supported projects on cybersecurity to improve cooperation in the industry, drive investments and spot trends.

Ferguson, a former teacher with a Master's degree in educational management, thinks cybersecurity in Europe is headed in the right direction. Greater attention and investment are going into it and a more European approach is emerging.

‘Cybersecurity is very fast-moving,’ Ferguson said. ‘Emerging technologies such as artificial intelligence and blockchain are important to watch. At the same time, any gaps in your capabilities can be dangerous.’

Research in this article was funded by the EU. If you liked this article, please consider sharing it on social media.

More info

- ECHO
- cyberwatching.eu
- Innovation and security research