Online security assessment framework helps businesses cope with increased use of personal devices

Employees increasingly access sensitive company data remotely, often from personal devices where social media networks hold a prominent place. Easy targets for cyber criminals? Members of the DOGONA consortium believe so, and they have devised a risk assessment framework to help businesses alleviate this threat.

© AngieYeoh, Shutterstock

Working anytime, from anywhere. This could easily be an advertising slogan for the increasingly widespread corporate culture of telecommuting. And who would argue against it? Working from home cuts down on company expenditures, increases productivity, makes employees happier, and even helps tackle issues such as congestion and CO2 emissions. But this new philosophy also does raise a few questions, a good one at that being related to security. Whilst industries have always been vulnerable to cyberattacks, the risk has considerably increased with the blurring line between private and professional devices, and the unprecedented success of social networks. As Ms Francesca Giampaolo, coordinator of the DOGANA project, explains, there are different factors at play. “Not only do people increasingly use personal devices for work purposes, but they will often combine this use with that of social media whose business model consists in encouraging them to reveal and share personal information. These platforms fail to provide strong authentication mechanisms and, to make things worse, many people seem unable to avoid subjecting themselves to unnecessary risk and lack the knowledge to efficiently secure their devices.” DOGANA answers this problem with a framework delivering ‘advanced social engineering and vulnerability assessment’ to measure and mitigate the risk related to social vulnerabilities. Whilst all industries are vulnerable, the system allows for quantifying actual risks based on business’ ICT dependence, level of consequences following attacks, level of associated risk and other metrics. The framework consists of an open source toolchain to perform the vulnerability assessment (information gathering, attack and hook preparation, attack execution and reporting); a training programme including awareness methods and a set of tools for automated risk mitigation; and a law enforcement component. According to Giampaolo, DOGANA’s main innovations include the ‘information Gathering framework’ which relieves testers from gathering the information on their own, in turn reducing error rates and improving efficiency. There is also the ‘awareness framework’ offering a range of awareness methods that can be tailored to the needs of a specific company; as well as the ‘organisational policy framework’ that will provide a set of guidelines and requirements specifically for European enterprises. DOGANA is also fully compliant with GDPR. “The framework is designed to provide general Social Driven Vulnerability Assessments (SDVA) services, but at the same time

specific parts are tailored for the four application domains of applications that have been tested in the trial phase (defence, government, transport and emergency),” Giampaolo explains. “Additionally, DOGANA has been designed with two distinct classes of end-users in mind, each with its own limitations and responsibilities: the SDVA Tester, responsible for tasks related to preparation and execution of SDVAs; and the Company Representative, who can access statistics and reports on the results of SDVA execution.” DOGANA is targeting companies whose employees use a computer daily, providing a solution that can help them monitor the percentage of these employees that get tricked by phishing and social-engineering attacks in general. “We will help these companies to provide training programmes to make sure that their employees fully understand how to avoid getting tricked by emails that look very credible to an inexperienced user,” Giampaolo says. Market offerings around DOGANA will include consulting services and training, and each consortium member will be promoting the framework to its relevant networks and partners.

Keywords

DOGANA, social media, security, personal device, company data, vulnerability assessment, framework