Crisis Averted? Xerox and Swascan Responsible Vulnerability Disclosure

On the sideline of what some have already called it the biggest ransomware attack in history, the Kaseya attack, Swascan and Xerox show how to properly mitigate third party risks through Responsible Vulnerability Disclosure

Italy, Milan, Jul 7, 2021 (Issuewire.com**)** - During an activity of security testing, through the Domain Threat Intelligence service, the Italian company Swascan (Tinexta Cyber) came across a series of possible vulnerabilities linked to the supply chain of the American giant Xerox.

The Norwalk (Connecticut) based giant has a turnover of 10.27 billion dollars and 24,700 employees. No company is a closed universe, and therefore protected: the hyperconnectedness and widespread digitization that has developed rapidly in recent decades have brought about a substantial change in the economy.

At Xerox, too, many activities are entrusted to third parties, whether they are consultants, partners, suppliers, or representatives/vendors. A digital supply chain, however, can present pitfalls for corporate cybersecurity. And the larger the perimeter, the greater the risks to an organisation's digital ecosystem. The case involving Xerox and Swascan is a case in point.

The Offensive Swascan Cyber Security Team identified at least two critical vulnerabilities on Xerox's

digital security perimeter. For example, it was not known that Xerox's web application was responding incorrectly to http requests by displaying its credentials, resulting in a vulnerability and thus allowing a criminal hacker to execute attacks. Likewise, the existence of a misconfiguration allowed a criminal hacker to take control of a victim's computer.

Once these anomalies were detected, Swascan immediately informed the American multinational company's security team using the Responsible Vulnerability Disclosure process. Promptly, Xerox's PSIRT, through its own investigation, discovered that both hosts were not operated by Xerox itself but were the result of a past or current business association with a third-party organisation.

Commenting on the collaboration between Swascan and Xerox, Pierguido Iezzi, CEO of Swascan, added: "This is a textbook example of how third-party risks are one of the most insidious areas of a modern Cyber Security Framework. Managing the extended perimeter is the key to efficient and resilient corporate cybersecurity. This is why the Supply Chain Cyber Risk Indicator activities together with the use of Threat Intelligence are essential to effectively assess the level of exposure of the extended enterprise ecosystem to Cyber Risks".

You can read all the details of the activity at this link

Media Contact

Swascan

f.giberti@swascan.com

Source : Swascan