



Malware solution helps reduce threats at government agency in Italy

Client name: National Institute for Insurance against Accidents at Work (INAIL)

Location: Rome, Italy

Industry: Public sector

Challenge

- Identify an effective solution to counter ongoing malware threats
- Make the workforce part of the detection system instead of the weakest link
- Simplify the process of contending with malware to improve productivity

Solution

- Identified Cuckoo Sandbox as an effective open-source malware analysis solution
- Developed sandbox broker framework to load balance sandbox instances and as a way to profile customer submissions through authorization keys
- Deployed malware-detection solutions to serve both technical and non-technical users

Results

- Significant strengthening of the agency's resiliency to malware threats
- Avoidance of costs related to malware infection and recovery
- Improved sharing of information with Italy's national computer emergency response agency

Malware attacks have wreaked havoc across the globe as cyber criminals take advantage of what is often the weakest link in enterprise security: users. Because the National Institute for Insurance against Accidents at Work (INAIL) in Italy provides insurance-related online services and processes a considerable amount of sensitive data, cyber security is of paramount importance. When malware countermeasures at INAIL were proving to be ineffective, the agency turned to DXC Technology to develop a new strategy.

DXC deployed an innovative cyber security solution for the government agency that significantly strengthens the organization's resiliency to malware attacks. The system lets INAIL employees self-test suspicious email attachments in a user-friendly manner, which has resulted in lower support costs and increased productivity, among other benefits.

DXC already had a strong presence at the agency, including an active engagement to help improve the security of INAIL's IT infrastructure. The key requirements for the malware solution: It had to be easy for employees to use, and it had to be possible to deploy it quickly within INAIL's existing ecosystem.

DXC's product expertise in malware and security operation systems served as a foundation to develop an on-premises answer that lets INAIL respond quickly to threats. Deep domain knowledge in malware and familiarity with the best open-source enterprise security software allowed DXC to develop an approach that has proved to be a good fit for the agency.

DXC built the system on Cuckoo Sandbox, open-source software that provides powerful malware analysis but was originally designed to be used by highly technical security experts. To make Cuckoo work for INAIL, DXC developed a sandbox broker framework to load balance multiple sandbox instances, and a way to profile customer submissions through authorization keys. DXC also implemented an email interface featuring a simplified malware analysis workflow that could serve non-technical users.

DXC deployed two versions of the solution: Maya, an external integration layer for technical users, and Horus, an easy-to-use, self-service malware analysis solution provided to INAIL's 11,000 users. Horus uses a simplified alert system to identify suspicious email attachments that users can forward to a central Horus address for analysis. It generates a report that rates the potential threat on a scale of 0 to 10. At the same time, it sends a feed to INAIL's security team so they can take appropriate action.

Better security, lower costs

Automation has been built into the solution. When a user submits a malware report, it enables immediate protection of other users. The tool also gives the INAIL security team visibility into malware attacks that are targeted specifically at the agency and have not been identified as global threats by security vendors.

Adoption of the DXC solution has provided many benefits to the agency. Since Cuckoo Sandbox is open source and has an active user community, INAIL doesn't have to pay licensing and support fees. And the system allows INAIL to more easily share security threat information with Italy's Public Administration Computer Emergency Response Team (CERT-PA), a government agency charged with dealing with cyber attacks. This has boosted INAIL's visibility and reputation as a leader in cyber security, and it supports the agency's strategic goal of becoming a national services provider for other public entities in Italy.

The introduction of the malware solution has also improved security awareness among INAIL employees. Users are no longer seen as a weak link and are actively involved in protecting the agency from malware attacks. INAIL has benefited from fewer security help desk calls and improved employee efficiency. By avoiding time spent on analysis and recovery related to malware, the system has reduced total costs associated with security incidents.

About DXC Technology

DXC Technology (DXC: NYSE) is the world's leading independent, end-to-end IT services company, serving nearly 6,000 private and public-sector clients from a diverse array of industries across 70 countries. The company's technology independence, global talent and extensive partner network deliver transformative digital offerings and solutions that help clients harness the power of innovation to thrive on change. DXC Technology is recognized among the best corporate citizens globally. For more information, visit www.dxc.technology.