Penetration Testing for Reconice to Improve ePHI Security

Case Study

Summary

ScienceSoft verified the IT infrastructure of a speech recognition software provider against vulnerabilities and conducted black box pentesting of their solution used at 500+ healthcare organizations to ensure ePHIs remained uncompromised.

Customer

The Customer is **reconice**, the leader of the medical speech recognition market in Italy. Providing software to 300+ hospitals and 200+ diagnostic centers, **reconice** was the first company in the country to offer an OS-independent solution with multidisciplinary medical vocabulary. Today, **reconice's** products allow physicians, surgeons, nurses, to create reports by dictating data, thus optimizing medical professionals' work time.

Reconice wanted to verify the security of their Dycendo speech recognition application and check their IT infrastructure against potential vulnerabilities and was looking for a vendor with a proven track record both in security testing and in healthcare.

Speech recognition application security testing

Bringing in vast experience in cybersecurity and healthcare IT, ScienceSoft's team devised a tailored plan and conducted black box penetration testing of reconice's speech recognition application Dycendo. Having limited information about the application, ScienceSoft's cybersecurity experts imitated a real-life hacking attack to reveal potential security issues. As a result, **reconice** got a list of the vulnerabilities and a thorough mitigation plan to improve the application's security and protect ePHIs created by its clients from theft, inappropriate use, deletion, etc.

IT infrastructure security testing

To check **reconice's** IT infrastructure against cyberthreats, ScienceSoft's cybersecurity experts carried out black box penetration without any information on the Customer's current security policies and network protection. As a result of black box penetration testing, ScienceSoft provided **reconice** with tangible steps towards risks elimination.

As employees may be a prominent cybersecurity risk factor, additionally, ScienceSoft's experts decided to imitate a phishing attack against the Customer's staff. The campaign helped **reconice** identify gaps in its employees' cybersecurity awareness, in particular, the ability to recognize and withstand social engineering techniques.

Marco Biraghi, CEO at reconice, says:

"*Italy has seen several high-profile cyberattacks recently; a stark reminder that security should not be just an afterthought. This is why we entrusted ScienceSoft to verify our application and organization against any weak points and vulnerabilities: to guarantee the highest levels of security and provide our clients with a solution they can rely on.*

Thanks to penetration testing conducted by the ScienceSoft team, we can now identify and act upon threats at an early stage, shielding our clients from even the slightest inconvenience."

Key outcomes for the Customer

- Created vulnerabilities elimination strategy and security enhancement plan.
- Increased client trust and satisfaction due to proactive security improvement.
- Improved cybersecurity awareness among the Customer's staff.