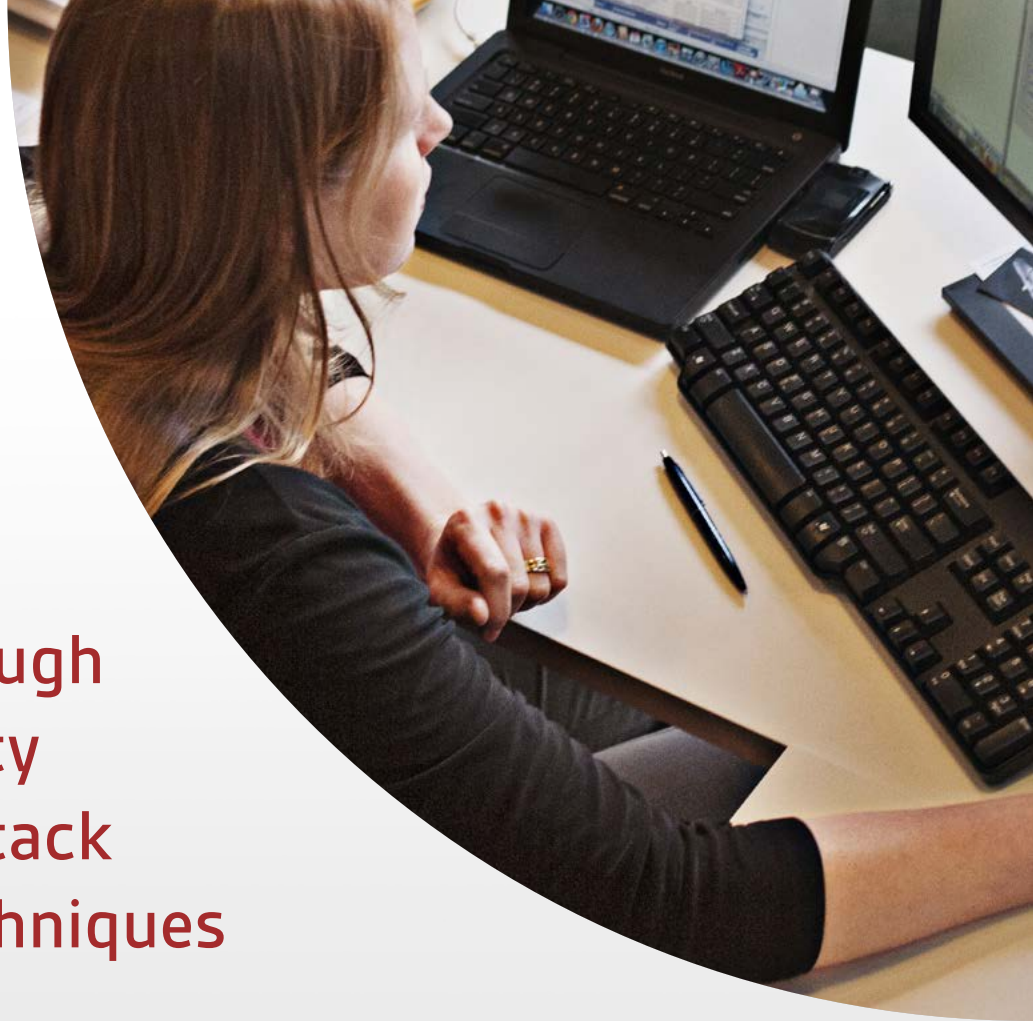


Gaining cyber resilience through layered security testing and attack simulation techniques

How BSI's attack simulation team helped a global financial institution to assess their prevention, detection, and response capabilities against the potential threat vectors targeting their network security by conducting a red team assessment.

In brief

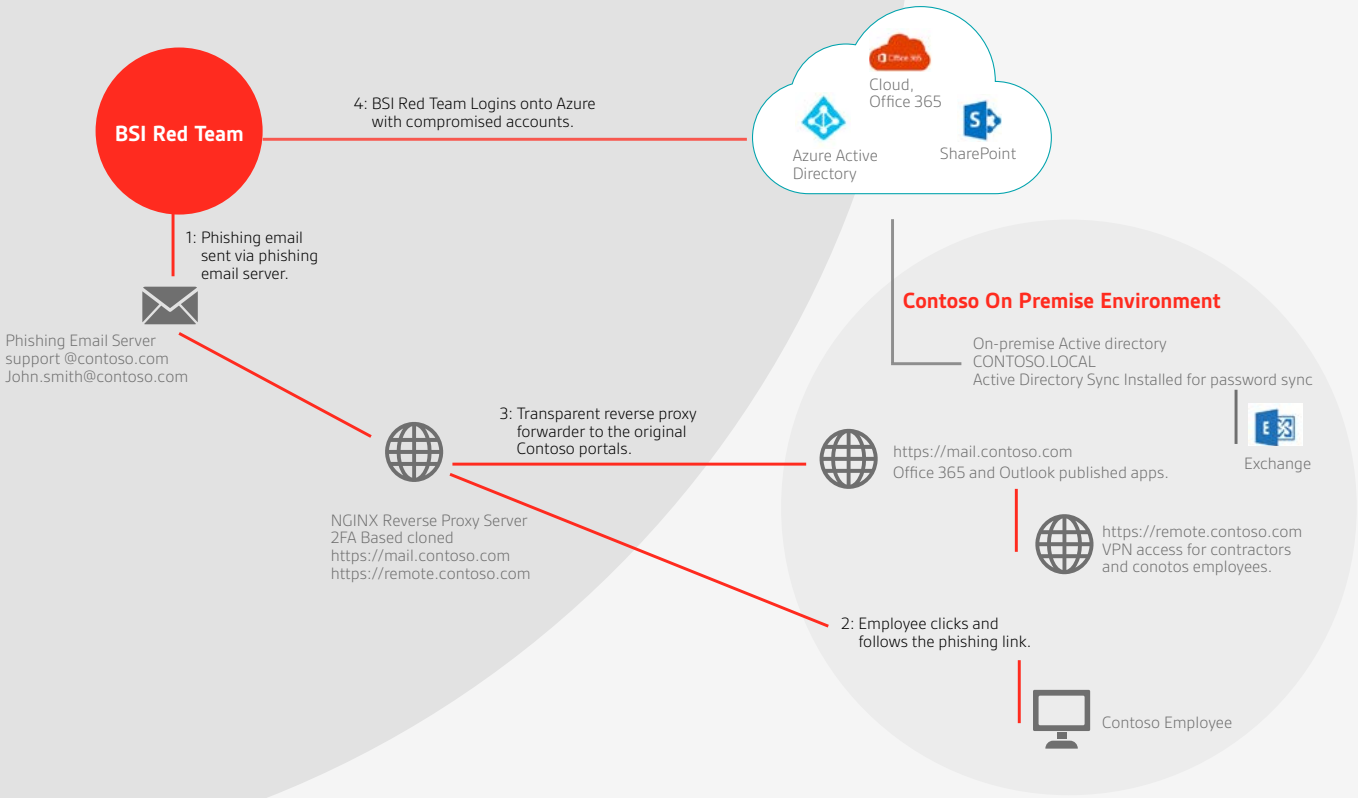
In order to simulate the likely root causes of potential cyber-attacks, BSI's red team were tasked with the objective to gain authorized access to a financial institution's internal network and applications. As the external perimeter of the organization appeared to have been securely hardened, BSI's red team targeted the organization's employees through social engineering attacks, mimicking the methodology and approach of a realistic attack against the organization.

The solution

To perform this exercise, the contact information of the organization's employees was harvested through reconnaissance exercises and targeted social engineering attacks were performed against relevant employees, with the attacks emerging from BSI's dedicated phishing server. These phishing attacks appeared to emerge from the organization's support and service desk functions, with links to a BSI controlled transparent reverse proxy. Victims of this attack were tricked into submitting their credentials to BSI's controlled proxy, which were then forwarded to the relevant, authentic portals, making the attack appear benign.

Contact us

IE/International
Call: +353 1 210 1711
Email: digitaltrust.consulting.IE@bsigroup.com
Visit: bsigroup.com/digital-trust



Once this phase of the exercise was completed, it was possible for BSI's red team to gain unauthorized access to the organization's cloud-hosted applications and VPN portals using the compromised credentials, achieving the objective of the exercise.

The benefit

Upon completion of this attack simulation exercise, it was evident that even though the external perimeter of the organization was securely hardened, it was still possible to gain access to the internal network through targeted social engineering attacks against employees. This exercise highlighted the scope for improvement in employee security awareness training and inadequate detection and prevention controls on the users' devices. In addition, one of the main outcomes of the exercises highlighted that even though multiple detection and response solutions were deployed, the red team's activities went undetected. After thorough investigation, it was discovered that some of the security solutions deployed on the network had been misconfigured, whilst others were not fine-tuned to the organizations expected security baseline, reducing the likelihood of detecting and alerting anomalous behaviour. In one case, one of the tools was correctly configured; however, an exception to all internal VLANs was applied, rendering the tool ineffective.

This outcome is something encountered on a regular basis during red team and purple team exercises. An organization would have a lot of tools in place to detect and respond to breaches and threats; however, these are often not utilized properly and, therefore, offer a false sense of security.

bsi.

Why BSI?

BSI's Security Testing Team helps organizations to secure their network from a potential malicious attack, verifying their current protocols, policies and procedures to keep information and data secure, safeguarding their reputation and ultimately, making them resilient.