Computest
always on.

Red Teaming example case

Simulating a real cyber attack

ACME wants to know if it would be possible for a malicious party to obtain the blueprints for their patented production process. ACME has already taken various security measures (such as pen testing and vulnerability assessments) and has been working with a security policy and an SOC for a year. Would these measures offer sufficient protection in a realistic situation in which a competitor was attempting to obtain their business-sensitive information?

We agreed with ACME that we would carry out a Red Teaming assignment over a one-month period. At the kick-off meeting for the assignment, the rules of engagement were laid down:

- We were permitted to use all available means; only attacks against the OT domain were excluded, so as not to disrupt the production process.
- Only the CEO and CTO were aware of the Red Teaming assignment, so that the attack would yield the most realistic picture possible.

Physical intrusion into the premises

We started with external attacks against ACME's IT infrastructure, but these were unsuccessful. Our ethical hackers then decided to attempt to physically penetrate ACME's premises. One of the hackers got in by following an employee through the smoker's entrance at the rear of the building. Once inside the building, he connected a device to a network port in the meeting room. The device had its own internet connection via 4G, enabling access to the internal network from the outside.

Access to the HR system

It was easy to get into ACME's internal network in this way, but how much further would we get? We managed to gain access to the internal HR system via the internal network because one of the employees, who we found on LinkedIn, had reused a password that had previously been part of a data breach. By exploiting vulnerabilities in the HR system, we were able to register our own man as an ACME employee. We also checked the ERT option.

Re-entering the company premises

Armed with a home-made access pass, one of our hackers walked back into the building – this time through the main entrance – and up to the ACME counter. He told the reception employee that his pass didn't work. Because he was now registered as an employee, he was given a temporary access pass. Once at the IT department, the hacker requested a new pass, which he was given without further question. Because he was registered in the HR system as a ERT member, he was even issued a personal pass giving him access to all areas of the building. After having a chat by the coffee machine, he continued on his way to the server room. The lock immediately accepted the new access pass. Our goal was to discover the administrator's password.

Discovering the system administrator's password

ACME's CTO had previously indicated that a certain amount of downtime for a particular server would be acceptable. The hacker therefore placed a small device between the keyboard and the server that records all keystrokes. He then switched off the server and quickly left the server room. After that, all we had to do was sit back and wait for a system administrator to turn the server back on and enter his password. Within 15 minutes we had it! Uh-oh, the password turned out to be a combination of his favourite football club and a year. Once we had the system administrator's password, it was easy to log into the file server from our office and so download ACME's blueprints. Mission accomplished.

Cyber attack: blueprints of ACME's patented production process stolen

The total estimated financial loss is €50.5 million, consisting of:

- Loss of value of international patent: €50,000
- Cost of lost R&D: €450,000
- Lost turnover due to increased competition: €50 million

info@computest.nl
www.computest.nl
+31(0)88 733 13 37