The Target Breach

Several of us at L4 Networks read with interest how the Target breach occurred. This newsletter, albeit longer than we would like, walks through some of the issues uncovered. It should be a wakeup call to all of us I.T. professionals.

Although there is still much that is left unanswered (or rather left vague by the heads of the company), hackers were able to get into Target's point of sale (POS) system by using a vendor's stolen credentials to get remote access into the heating, ventilation and air-conditioning (HVAC) remote control system. Once in, they were able to burrow into other systems, including the POS system.

They were able to do this easily because HVAC companies are often granted network access to clients so that they can monitor and diagnose problems remotely. This is quite common and quite broad for the ever increasing amount of Internet connected systems (e.g., phone, alarm, fire, HVAC, power, SCADA, etc.).

The problem was not so much the remote access but the fact that too often vendors, due to lack of proper security technology, creativity and patience (usually all three), use the same credentials across multiple companies. Thus, once compromised at one company, hackers have the password to multiple companies.

Moreover, in Target's case, their HVAC systems were apparently connected to the same subnet as their POS. That is simply poor or lazy engineering. Such control systems should be isolated from each other and from the production networks via firewalls and be provisioned on separate subnets. Vendor and employee access needs to be logged, actively monitored, and secured by strong and frequently changed passwords and used in conjunction with multi-factor authentication methods

Many companies have no idea how many of their systems are "visible" online. Most I.T. infrastructure growth is bolt-on without an eye to the security architecture and the potential risks they are introducing with each new addition.

A further piece of information that leaves many of us in the dark with respect to Target was that the company said it passed a security audit before its breach last November. That makes one wonder how in depth and how competent this audit was, when exactly it took place, and if any of the resultant recommendations were actually implemented or simply shelved by the bureaucrats.

The payment card industry's data security requirements outline how employees, administrators and vendors can remotely connect to systems. They require merchants like Target to employ multi-factor authentication, which adds a second, temporary password during the login process for employees, administrators and vendors trying to gain entry to their systems remotely. Target would not say whether its vendors were required to use multi-factor authentication or had access via VPN technology (which creates a private tunnel between employees and vendors working remotely and the company's private corporate network). If it was the latter, i.e., VPN, then clearly their network engineering was extremely poor.

At L4 Networks we have helped several of our customers tackle similar problems. One example is an organization in the medical field that needed vendor access (labs, pharmacies, etc.), several remote site-to-site access points, provider access from home, and I.T. support access. Using solid and secure

engineering designs, remote access appliances, and a solid and well managed firewall, there has been never been a breach in the four years since the project was completed.

If you are looking for an I.T. company that can provide solid network engineering, secure multi-factor authentication, remote access appliances and top quality firewalls, and has the skills to manage and monitor these systems then look no further than L4 Networks.

We have been in business for 25 years and have built a solid reputation as experts in I.T. infrastructure and security.