Dynetics

Vendor Persistent Threat:

Vendor access to corporate networks is an all-too-real security risk

Apr 22, 2014

In real world security assessments, it is common to find that firewalls implemented to secure different zones are misconfigured as a result of poor security policies or outsourced IT integration, or troubleshooting "fixes". The vendor that supplied the firewall either did not truly understand the firewall technology being implemented or did not perform systems engineering requirements analysis to determine how the firewall should be configured. These firewalls are essentially functioning as nothing more than routers forwarding traffic between zones due to the lenient security policy implementation that evolved over time. These issues with firewall security are becoming more and more common as a result of the position technology has taken in business functions. Security policies have not adapted to this growing trend, which has opened the door to threats penetrating your network from an unlikely source, a vendor. Dynetics refers to this kind of security risk as the Vendor Persistent Threat (VPT).

Most vendors have trusted relationships with the companies they support. Vendors typically require remote access into customer network to enable easy access for tech support, such as troubleshooting, applying patches, and performing updates. The remote access may be over a dedicated VPN, on-demand VPN, SSH, or possibly dial-up in some legacy systems. In the scenario of a dedicated VPN, attention must be given to insuring that the vendor can only access systems that are needed to meet the terms of the service contract. The local IT infrastructure must be configured against horizontal and vertical pivoting within the network. Detailed system event and network flow logging is required to insure trusted access is not exploited. The risk of a vendor network being compromised and, in turn, being used as a pivot point for exploiting customer network trust relationships must not be overlooked. Similarly, if a vendor's technical support team can be identified, they may be directly targeted with the end goal of compromising individuals with remote access credentials and sensitive information for how numerous customer networks operate.

Dynetics, through years of conducting security assessments and Network Architecture Reviews, has observed holes in the firewall, lingering vendor accounts, and VPN connections that are established from outside of the enterprise. These issues are what we refer to as the vendor persistent threat. Although Dynetics recognizes the real need for vendors to provide remote support to an enterprise, it is still the enterprise's responsibility to secure that access.

Dynetics recommends regular firewall reviews, time-based access for vendor-performed functions on the enterprise network, and policies and procedures that begin at the point of purchase so that the right terms and conditions are written into the contracts. Most importantly, implementation of two-factor authentication so the customer organization holds the access and grants access only after verifying the vendor is authorized to access the network. For more information on vendor persistent threat, contact one of Dynetics security experts at 256-713-5010.