Herding Cats:
The Perimeter has Left the Building

August 2009

BrandenWilliams
SECURE BUSINESS GROWTH

For those of you who have been in this business for more than ten years, think back to what the network you managed looked like in the mid-90s. Internet connections usually terminated into a router that was connected to a firewall with two "protected" zones: a DMZ and your internal network. Sound familiar? I managed a few networks nearly identical to that. Where was the perimeter? Right! At the firewall or potentially your border router, depending on what it was doing for your network.

Even in large corporations, older network designs typically had a single point where you could put your finger on a network diagram and say, "Yep, there's the perimeter right there. Point the heavy artillery in that direction." Companies with multiple sites often used frame-relay technology and had massive frame clouds connecting all of their locations together to some termination point behind the main firewall. Not until the last five years have companies heavily leveraged VPN technology to connect their various locations. Even today, most companies only use VPNs to connect individual users and small remote sites, such as stores or small satellite offices, to the corporate offices. Larger sites still connect via frame relay or wide-area Multiprotocol Label Switching (MPLS) networks.

With the cost and quality of bandwidth increasingly demonstrating their inverse relationship[1], more companies are choosing to install business-class Digital Subscriber Lines (DSL), cable, satellite, wireless, and other types of pro-sumer grade network connections. Convergence in the perimeter security market now means that a satellite office with ten users can transparently communicate with the corporate office through one single device.

But what does that mean for that point on the network where we put our finger?

In most networks I review, that "point" doesn't exist anymore. Compliance initiatives with network segmentation incentives to reduce scope yield enclaves where certain systems live. It's much easier to pick one compliance initiative, or one particular context, and ask someone to point out its network perimeter. But even those can be complex when you add in semi-trusted connections from ExtraNets or partner VPN connections.

What do you do now? Your charge is to prevent a data breach with 50% less budget and probably the same cut in staff.

First off, throw the concept of a perimeter into the coffee grinder and switch it on to powderize. It's gone the way of the DEC Multia[2]. The next step is a hard one. In order to protect data effectively, you have to know where it lives. You can either deploy the digital bloodhound of your choosing (commercial or open source), or you can make some educated guesses on where the data probably lives, and focus on protecting that.

While door number one above is the most logical step, your reduced budget and resources may prevent you from effectively carrying that step out. Door number two is definitely a second choice, but if you focus on some key areas of your infrastructure, you can create extremely effective controls in spite of the vanishing network perimeter.

FOOTNOTES

[1] Meaning that the cost goes down while the quality or amount of bandwidth you get for that cost is going up.

[2] Man those things were cool!

The following is an abridged list of buckets that most of your enterprise's key infrastructure components can be placed into:

Workstations: Nobody wants to think about it, but they are the biggest source of data leakage we all face.

Application Servers: Internal application servers sometimes are right behind the "new perimeter."

Database Servers: Sometimes housing the keys to the kingdom, these servers should be treated differently than the internal application servers.

Internet Servers: External application, Web, DNS, and email servers that communicate with the Internet must be isolated from the internal infrastructure.

Finally, a few groups of users to consider—each having different access needs: Employees (which should be broken into subgroups), internal non-employees (like contractors), and external users (customers, partners).

Once you have defined your key areas, it's time to deploy protection to these devices. Software-based firewalls are an effective tool to create mini-perimeters specifically on key systems. Most desktop anti-virus solutions have this capability. For servers, re-deploying firewalls and access lists in routers and switches is appropriate. Application-based firewalls come in appliance and software form, but can add additional protection.

Face it, you cannot rely on the external perimeter anymore. It's time to view the perimeter as a relic of the past, and re-deploy your security to combat the sophisticated inter-connected networks of today!

About the Author:

Branden R. Williams, CISSP, CISM, CPISA/M, has been making a name for himself in the Information Technology and Security arena since 1994, as a high school Junior. Now, a graduate of University of Texas, Arlington earning his BBA in 2000 with a concentration in Marketing and the University of Dallas, where he earned an MBA in Supply Chain Management & Market Logistics, in 2004, Williams is sought after as both an Adjunct Professor and Information Technology & Security Strategy Leader in the corporate world.

Williams regularly assists top global retailers, financial institutions, and multinationals with their information security initiatives. Read his blog at or reach him directly at http://www.brandenwilliams.com/.

TEL 214 727 8227
FAX 214 432 6174
BLOG brandenwilliams.com
EMAIL brw@brandenwilliams.com

brandenwilliams
SECURE BUSINESS GROWTH