# Security is not a luxury item

**Lori MacVittie, 2008-08-12**

In the face of a recession everyone, individuals and organizations alike, begin scaling back spending. The first thing to go is luxury items; after all, you probably didn't ***need*** that big screen TV for Christmas, and the kids will likely be just as happy with used video games as they would with new ones.

IT departments quickly scale back as well, putting off larger, more costly projects that aren't critical to the core business and re-evaluating much of their infrastructure in an attempt to cut costs and reduce the impact of the hardware and software costs of running a modern business.

Unfortunately, many organizations consider security a luxury item instead of a necessity. The trick is in determining what is needed and what is not, and unfortunately this is often where the inability to quantify security risks in terms of hard dollars results in a scale back of security.

Greg Mechback at Network World Canada expressed it well in a recent blog post:

> *Budgeting for security can be tricky. You need to separate what's actually required from products that the lawyers say you need to exercise "due diligence." For example, anti-spam and "compliance" software tends to fall under the realm of security, but this raises a few questions. Will your company fail to operate if the CEO gets five e-mails from entrepreneurs trying to sell him Viagra? Does your company need to save every single file and e-mail, even those that send 5 MB PowerPoint presentations that would not be as critical as financial transactions in the event of an investigation?*
>
> [...]
>
> *But if you're company is suffering a loss of business, cutting back on security in the wrong areas could make a bad situation worse.*

The key concept here is really about trying to measure the ***real*** risks of cutting back on security and determining what is necessary protection and what isn't. You have to ask yourself "Can we afford ***not*** to have this security in place" before cutting it from the budget.

One security option that is often seen as a luxury item is a web application firewall. After all, you have plenty of other security solutions in place that scan, examine, and scrutinize requests and responses as they flow in and out of your data center, and certainly that makes a web application firewall redundant. It's a luxury, isn't it, that you can certainly afford to go without it.

No, it's really not. Sure, an out-of-band IPS can probably detect that there is a malicious payload in that HTTP reply, but by the time the IPS notices it, it's already too late. The client has already received the reply and been compromised. And that network firewall may be able to detect and stop a layer 4 DoS (Denial of Service), but it isn't going to even notice a layer 7 DoS, which can bring online transactions to a screeching halt.

You could also decide that you'll just modify your applications to detect attacks and that's certainly an option. But don't fool yourself into thinking it's a less costly option. Developers still have to be paid to modify the application, and time has to be spent coding, testing, and deploying. And in the mean time, you're vulnerable to attack.

Perimeterized security for web applications makes even more sense if you're employing virtualization technology to consolidate servers in an effort to reduce costs. A single attack targeting the operating system or virtualization layers on one server could potentially bring down multiple, business critical applications. Detecting and preventing that attack at the edge of the network using a web application firewall simultaneously protects ***all*** applications running in virtualized containers on a single server and by offloading security functionality improves the capacity of the server as well.

Security is almost never a luxury item. In times when budgets are tight, the trick is not only to determine what's necessary, but also to squeeze the most functionality out of every investment. A web application firewall protects multiple applications across multiple layers of the network and application stack. A web application firewall cuts down on software and licensing costs of distributed security solutions that require deploying solutions on every server or to be integrated with every application. And by stopping attacks before they can even get close to your applications there is less chance that something nasty will sneak through and drastically increase your spending with the time and effort needed to clean up the mess. Stopping an attack at the edge can prevent the compromise and infection of one application that spreads to others in what is nearly an exponential growth pattern.

The first line of security in your home is always at the point of entry: on the doors. It make sense, then, that the first line of application security should be at the perimeter in the form of a web application firewall. You may be able to do without the expensive, internal motion detecting system but the security at the door is something you really can't afford to do without.


Related articles by Zemanta

- Which security strategy takes more time: configuration or coding?
- Secerno and F5 hook up on network security
- Is Your Network Secure?
- Layer 4 vs Layer 7 DoS Attack



F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

| F5 Networks, Inc. | F5 Networks | F5 Networks Ltd. | F5 Networks |
|---|---|---|---|
| Corporate Headquarters | Asia-Pacific | Europe/Middle-East/Africa | Japan K.K. |
| info@f5.com | apacinfo@f5.com | emeainfo@f5.com | f5j-info@f5.com |