When Everything is a Threat Nothing is a Threat

Lori MacVittie, 2010-05-03

The current threat level is … the same as it was yesterday, and the day before, and will be tomorrow.

We've all been in the airport before and heard the announcement. "The current threat level is orange. Blah blah blah blah yada yada whatever." At least that's what I hear today because I've become immune to the fact that "orange" means there's a threat. There's *always* a threat, it seems, and the announcement simply conveys what appears to many of us to be the "status quo." We have effectively been desensitized to a "higher" threat level as it is now treated as nothing out of the ordinary. It is the norm, rather than something that grabs our attention.

The same is true in the enterprise, where the threat level is always high. Although most organizations likely don't have a "threat level announcement" the effect is the same: personnel and infrastructure alike treat this allegedly "heightened awareness" as the status quo. It's no longer actually heightened, or more aware, it's the way it always is. Many times this is because there's always a credible threat to the infrastructure and applications of any organization. At any time there may be an incursion, an attempt at penetration, the exploitation of an old or newly discovered vulnerability. This forces information security teams to put into place the infrastructure and solutions, both active and monitoring, that will detect and (one hopes) prevent a successful attack. These solutions are ***always*** on alert, twenty-four by seven, three-hundred sixty-five days a year.

The problem with always being at a “heightened” state of security awareness in the infrastructure is twofold. First, real threats may go unnoticed amongst the hundreds of other “alerts” about anomalies that aren’t truly attacks. Out of the hundreds of failed log-in attempts in any given day how many of them are actually attempts at hijacking an account and how many are just attempts by legitimate users that forgot or fat-fingered their password? In many cases the determination of which is real and which is simply a case of user-error are left to a codified “process” that ends with a locked out account and, more often than not, a call to a help desk or an e-mail explaining the situation. Second, if every piece of infrastructure is always configured to be in “ultra paranoid” mode, it impacts the performance of all applications delivered through that infrastructure because the components are always expecting every packet to be “the one” that’s truly dangerous.

A dynamic infrastructure, enabled by Infrastructure 2.0, however, might resolve this problem – or at least give us the means by which we can architect an infrastructure that can.

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

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com