White Paper

The Psychology of (In)Security

Security Myths Create Risk Adversity to Change

Bromium®

Executive Summary

"The most high-profile data breaches were at organizations that failed to make the proper investments to properly protect their critical data from breaches."

When we consider the most high-profile data breaches of the past few years it should be alarming. The most high-profile breaches have all been at multi-billion dollar organizations, yet they failed to make the proper investment to properly protect their critical data from breaches. They failed to make the proper investments because they were afraid to make any substantial changes. It is basic human nature to fall into a routine, so nothing changed for these organizations, even as the threat landscape changed around them. It has been said that the definition of insanity is doing the same thing and expecting different results.

These breaches have resulted in lost trust for these organizations, lost value for their shareholders and have lost jobs for those responsible for protecting this critical data. Each year, organizations will spend $75B investing in security solutions, yet the frequency and magnitude of breaches continues to grow. The problem is that organizations are investing in the "status quo" by continuing to purchase and deploy legacy security solutions that are incapable of addressing the reality of the threat.

The challenge for security professionals is that the majority of security vendors trade on fear, uncertainty and doubt (FUD) to sell solutions that inevitably fail. When these solutions fail, security vendors turn to two common excuses that are perpetuated as myths. These two pernicious myths that security vendors spread are to "assume compromise" and that "sophisticated" attack cannot be defeated with existing security solutions.

Myth #1: Assume Compromise

When you walk the floors of industry trade shows and speak with security vendors, one of the most predominant endpoint security myths is “assume you will be compromised.” Bromium customers know this is a fallacy, but as a result of this axiom, the security industry has remained obsessed with post-breach detection, but at the cost of less protection.

The reason this myth persists is because “assume you will be compromised” is a self-fulfilling prophecy. If you believe you will be compromised then you will make investments in detection and remediation, instead of considering more effective forms of endpoint protection. It is a vicious cycle: assume compromise, invest in detection, compromise occurs because of inadequate protection, successful attacks are detected, and incorrect beliefs are validated. Repeat into the next budget cycle.

Myth #2: Advanced Attacks Are Too Sophisticated to Be Stopped

Sophisticated attacks present a significant hurdle for legacy endpoint protection. Sophisticated attacks may incorporate malicious websites, email or documents that have been developed to evade detection. Therefore, even diligent security teams may not be alerted to a compromise.

Additionally, continuing technology trends, such as cloud computing and mobile employees are relocating corporate assets beyond the corporate perimeter, increasing the need for effective endpoint protection. When a mobile user connects to an untrusted network, it is imperative that attacks don’t slip through the cracks.

Beyond the sophistication of attacks, there is also a balance between security and operations. Primarily, operations are concerned with ensuring that an organization remains productive, while security is concerned with compensating

"Compromise will occur if organizations continue to invest in detection instead of protection."

for vulnerable technology. For example, an organization may have developed its own legacy application that uses outdated and unpatched versions of Java to run, despite the obvious security vulnerabilities.

Therefore, an effective endpoint protection solution must be able to securely enable both legacy applications and new computing models from sophisticated new attacks without breaking them. Protection is not enough if we are not also maintaining a great user experience.

Adapting to Change: Fixing a Broken Model

There is an old saying in corporate America, "No one ever got fired for buying IBM," because IBM was trusted as the leader. If it isn't broken, then don't fix it. The problem is that security is broken; it only appears to be "working" until the next major breach. It is critical to understand that the majority of information security solutions do not work as advertised.

The reason it seems like endpoint security is a losing battle is because the current security model is broken. For example, the NIST Cybersecurity Framework organizes five basic cybersecurity functions: identify, protect, detect, respond and recover. Three-fifths of this framework (detect, respond and recover) assume compromise will occur.

Of course, compromise will occur if organizations continue to invest in detection instead of protection. Perhaps the only reason your organization hasn't made the headlines is because it is lucky enough to avoid attention. Or perhaps it has been breached, but it hasn't been detected. The security industry will sell $75B of products that will inevitably fail.

We must realize the psychology of our insecurity. Government regulation and industry mandates are not enough. Security infrastructure must provide a foundation that is secure by design because there is no army of security professionals large enough to analyze and respond to the haystack of alerts, looking for the needle of the attack.

"Security infrastructure must provide a foundation that is secure by design."

The reality is that many CIOs and CISOs know that the technology they use to secure the enterprise will fail them, but they don't know how to succeed. The answer is to adapt to change. Adopt new technology initiatives that do not fall victim to the security fatalism of "assume compromise." Those are the stories of security professionals that are indulging in their failure.

Your organization can be secured quite simply: use micro-segmentation to isolate your networks and applications. Ensure all your PCs and mobile devices are "untrusted"—even if they attach to your network directly—by ensuring that they access your applications from a separate network segment. Virtualize your data center, and micro-virtualize your PCs.

ABOUT BROMIUM

Bromium has transformed endpoint security with its revolutionary isolation technology to defeat cyber attacks. Unlike antivirus or other detection-based defenses, which can't stop modern attacks, Bromium uses micro-virtualization to keep users secure while delivering significant cost savings by reducing and even eliminating false alerts, urgent patching, and remediation—transforming the traditional security life cycle.

Bromium, Inc.
20813 Stevens Creek Blvd
Cupertino, CA 95014
info@bromium.com
+1.408.213.5668

Bromium UK Ltd.
Lockton House
2nd Floor, Clarendon Road
Cambridge CB2 8FH
+44.1223.314914

For more information go to www.bromium.com
or contact sales@bromium.com

WP.PsychSec.US-EN.1510