

Breaking the cycle of cyber breaches

Finding the right mix of security tools involves being flexible and focusing on outcomes



Patrick Sullivan

Senior Director of Global Security Strategy,
Akamai

WHEN WE LOOK back at cybersecurity breach reports compiled by leading vendors over the past several years, we see many of the same trends repeating themselves, which highlights the need for new security strategies.

At some point in a successful breach, there is easy lateral movement on the part of the attacker across an internal network. One effective way to break that cycle is by shifting to a zero-trust model, which removes trust and security from the network level. Zero trust is an architectural change that involves basing security decisions on a user's identity, strong authentication of that user and a keen understanding of his or her role. Based on these criteria, security teams can limit access to applications to the minimum required to perform the duties associated with the role.

There are many other innovative tools and strategies available. Unfortunately, they often require a great deal of expertise and time to configure properly and then continue to fine-tune. That consumption gap can be a challenge for agencies, which is why it's often best to give consideration to ease of use when choosing new tools. In other words, agencies should consider picking tools they have the resources to run or can quickly develop sustainable expertise in maintaining.

Agile, automated security

Conversely, some security analysts say the model of continually buying the latest security appliance from a vendor without ensuring that the customer has the expertise to keep it operating efficiently

has probably reached its conclusion. Now we'll see more agencies and private-sector entities buying products along with the expertise to run them as a managed service.

In terms of internal development, DevOps or a similar agile method is becoming mandatory if agencies want to stay ahead of adversaries. At Akamai, we see attackers scan on a massive scale for the existence of vulnerabilities — often within an hour of a vulnerability being revealed. Using DevOps could help agencies win the race to eliminate

vulnerabilities before an adversary can exploit them. Under a waterfall development model, it could take agencies several months to issue a fix. That is simply too long.

Agencies need to be extremely agile to stay ahead of vulnerabilities, and as they move to models that are heavily based on automation and DevOps, their security tool updates also need to be automated.

If developers must exit their workflow to manually update a security solution, it undermines the agency's ability to be fast,



DevOps or a similar agile method **is becoming mandatory** if agencies want to stay ahead of adversaries.

efficient and innovative and could expose it to new vulnerabilities.

Going beyond the AI hype

There is a great deal of hype about artificial intelligence and machine learning, and in some ways that hype overshadows the value of those solutions. For agencies, narrowing machine learning down to focus on a very specific problem can be extremely

beneficial. For example, the technology could support agencies' security efforts by examining data that is often overlooked.

The typical agency has reams of data making its way to a security information and event management system or a log graveyard. Better inspection of all that data by a machine learning algorithm could offer unexpected insights and free highly trained security experts for higher-level activities.

Ultimately, emerging cybersecurity approaches are about choosing tools that fit into an agency's automation flow, buying an outcome rather than just an appliance and using flexible approaches to help agencies respond more quickly to a continual flood of new vulnerabilities. ■

Patrick Sullivan *is senior director of global security strategy at Akamai.*

**SECURITY THREATS MAY CHANGE,
BUT AKAMAI'S ABILITY TO STOP THEM DOES NOT.**

Cyber security in a hyper-connected world requires enterprise protection at the Network, Application and Data Center.

Come see why the majority of the cabinet-level departments and all branches of the US Military trust the Akamai Threat Intelligence platform at carahsoft.com/IIG-emerging-cyber/akamai

Akamai