Blogs
August 09, 2024
Cybersecurity for Lawyers: A Series

If you are an attorney covering cybersecurity, not only do you have to stay on top of ever-evolving legal obligations and risks, you have to be able to speak competently with your technical counterparts.

Introduction

While there are plenty of technical resources, very few are geared to the needs of cybersecurity counsel. With that said, our goal in this series, “Cybersecurity for Lawyers,” is to talk through a variety of cybersecurity topics and issues of the day, with a particular focus on providing the relevant basics and practical context around complex technical issues for in-house counsel who handle cybersecurity issues.

In this first post in this series, we talk broadly about the concept of Zero Trust (and royal food tasters), which is a term you may see come up a lot in the cybersecurity arena. Zero Trust is not a specific tool, product, or solution, but rather a security philosophy that “assumes the breach” and therefore justifies the expenditure of resources that wouldn’t be required if your perimeter were completely secure (because it can’t be). At the same time, there are many different ways to implement a Zero Trust framework, and some are better than others depending on the specific organization and scenario.

Please feel free to send an email to Andrew Pak to suggest any topics you would like us to cover.

Cybersecurity for Lawyers: Zero Trust and the Plight of the Royal Food Taster

You are the head of security for the new empress, in charge of meals. You’ve learned from your predecessor, no longer alive, that you can’t always trust your cooking staff because the last monarch was poisoned. You devise a new security protocol that includes terminating the entire kitchen staff and house staff immediately and bringing in a new pool of trusted employees who will be vetted with background checks, psychological profiling, and months of surveillance prior to hiring. You present your plan, and the empress asks, "But how can we trust the people who do the hiring? How can we ensure someone doesn't masquerade as a vetted hire?" You respond with silence, causing the empress to shake her head and say, "You are missing the problem; there's the potential for security breaches every step of the way even if we've vetted these people at the beginning of their employment! So, I have a new title for you: Royal Food Taster. I hope you are hungry and have a strong stomach."

The empress is focused on Zero Trust. She does not assume that the people in her kitchen can be trusted—even if they were well vetted at the door—or that the food placed before her is the same that her kitchen prepared. She therefore wants you to **Never Trust, Always Verify.**

Principles of Zero Trust

Many products and services incorporate the term "Zero Trust," but there is nothing proprietary about the term—it refers to a security strategy for protecting networks. If you've heard the phrase "assume the breach," then the concept behind Zero Trust will be familiar. Unlike traditional security models that assume that users within an organization's network are trustworthy, the Zero Trust model of security fundamentally relies on "never trust, always verify." The Zero Trust security strategy focuses on enforcing security policies on each user, device, application, and piece of data, rather than protecting only the network perimeter.[1] As Zero Trust security systems become increasingly popular within organizations, it is important to understand the ins and outs of Zero Trust and the opportunities and implications of the security strategy. While this article is not meant to survey all of the definitions of Zero Trust available, these are some core principles:[2]

1. **Continuous Explicit Verification**. Zero Trust intentionally makes all network systems and assets requiring protection inaccessible by default. Every user, device, location, and workload requiring protection must be authenticated and authorized, based on all available data, prior to accessing any resource.
2. **Least Privilege**. In a Zero Trust system, each user and device has "least-privilege" access to an organization's resources. Each user is given the minimum level of permission required to complete a task and must request additional permission to access further resources, minimizing users' (and potential threat actors') exposure to sensitive parts of an organization's network.
3. **Assuming the Breach**. Zero Trust assumes that hackers have already breached an organization's network. Thus, actions to minimize the scope and reach of an ongoing breach are a key strategy. Because Zero Trust assumes attackers are both inside and outside of the network, organizations using the Zero Trust security model may implement a variety of breach minimization tools, such as segmentation, microsegmentation (making it more difficult for a hacker to traverse across portions of the network), threat detection, data encryption, and multi-factor authentication (MFA), which are all examples of practices that support a Zero Trust security model.

While an organization may appropriately employ some or all of these strategies, they are all supportive of a Zero Trust strategy because they assume that threat actors can bypass the security perimeter, and are mechanisms to search for or mitigate malicious internal activity within that perimeter.

Examples of Zero Trust Strategies

MFA in many ways exemplifies the core principles of Zero Trust because it adds an additional authentication check even after a user presents an accurate login and password. But beyond the implementation of a single control, a Zero Trust model would include multiple ways to gauge the overall likelihood that a particular user account is controlled by a malicious actor. For instance, while not a guaranteed sign of malicious versus non-malicious activity, an organization may add additional security checks to any device that attempts to log in outside of normal working hours or from an unusual geographic location, or look for other user activity that suggests malicious intent. While these sorts of checks do not guarantee that a particular user is who they claim to be, they are examples of the layers of additional checks an organization could do on an account that has already passed an authentication challenge, and they are therefore consistent with Zero Trust principles.

A Broad Range of Controls Can Support a Zero Trust Strategy

Many controls and tools can accurately be called consistent with Zero Trust principles, but some security checks are more effective than others. Take, for example, the plight of our Royal Food Taster, who has to taste a monarch's food for poison. That is a form of Zero Trust. The food taster would argue that there are other forms of Zero Trust, such as monitoring all the people who come in contact with the food, monitoring the food itself at all times, or announcing rewards for tips regarding assassination attempts. The food taster would be right in some sense, because instead of trusting that the kitchen staff are all loyal subjects based on the vetting process, it assumes any one of them can have malicious intentions. But while all of these practices employ a Zero Trust strategy, unfortunately for our food taster, some practices are more effective than others. In the same way, Zero Trust controls come in many varieties, with some being more effective than others. Nevertheless, an effective Zero Trust strategy layers many controls to reach a desired effect. While the use of a food taster may be the most effective check available at the time, when dealing with something as important as the life of the empress, a good strategy would be to also employ the less drastic measures (e.g., vetting, monitoring), thus providing a layered approach to security and perhaps saving a few food tasters.

The thing to remember about Zero Trust is that it is a strategy, and a very broad and amorphous one at that—not a specific tool, product, or even control. Anything that amounts to a form of control of verification on an already authenticated user is arguably Zero Trust, but that doesn't make that control in and of itself a good or bad idea for a particular organization's security posture, or otherwise convert the entirety of its cybersecurity program into a Zero Trust architecture. There are controls within a Zero Trust framework that might make sense for one organization but not another. And some of the tools that use the term "Zero Trust" in their branding and/or marketing materials would actually represent a downgrade in security if used by certain companies. If someone tells you their organization employs Zero Trust controls, that means nothing on its own because there are so many different ways to layer, configure, and implement these controls. Don't get us wrong—the development of Zero Trust principles has been incredibly important to improving cybersecurity writ large. But its main value is its recognition that there is no such thing as a perfectly secure perimeter, which serves as a foundational assumption for a good cybersecurity program.

The authors wish to acknowledge Summer Associate Laurel McCabe's contributions to this blog.

---

[1] *See* Zero Trust Architecture | NIST.

[2] *See* What is Zero Trust? | Microsoft Learn; *see also* Zero Trust Architecture | NIST.

Authors

Explore more in

Privacy & Security Data Security Counseling and Breach Response