SECURITY EVOLVES TOWARD ZERO TRUST

There was a time, not very long ago, when nearly all the work of an enterprise was done inside the enterprise in facilities under its control. Except in the hands of a rare bad actor, the organization's data was pretty secure. But with the rise of the internet, business activities moved out from the enterprise, often performed by mobile employees and customers, and security has become much more challenging.

"The farthest reaches of the enterprise network are the most difficult to defend," says Dr. Chase Cunningham, principal analyst at Forrester Research. "Organizations give laptops or phones to their employees, or worse, they let them use their personal devices. The fact that the edge is constantly shifting [moving the organization's access devices from a central location outward] requires organizations to strategically operate differently to have any chance of making a difference in their defensive posture."

Movement away from a centralized, strongly protected core has made enterprises and government organizations more vulnerable to attack than ever before. Hackers and the "bad guys" who want to do damage or to commit data theft or financial crimes—or merely to earn bragging rights about being able to break security at a prime target—have developed tools that have often stayed several steps ahead of the tools that were meant to intercept and prevent the attacks.

PROBLEMS WITH PASSWORDS

Computer security has been modeled on a "technology" that's thousands of years old—the password. The password was used to gain access to protected areas like fortresses and military camps. A messenger approaching the fortified area would be asked for a password. If he got it right, the messenger would be allowed to enter. Getting it wrong could cost the messenger his life.

For computer security, user names and passwords have been a primary method of "proof" that the person attempting to get into a system was authorized to enter. Although password rules have evolved over time—from just a few characters to complex passwords following an increasingly human-unfriendly set of rules (minimum length; mixed use of upper case and lower case; mix of letters, numbers and special characters; and a short expiration date)—a wide array of problems with this method of authentication remains.

The messenger who guesses (or perhaps knows) the correct password gets past the security barriers. Once inside, in many cases, the messenger gains full access to the resources inside the gate—or to all areas of the corporate network.

Whether the individual or machine that correctly enters a user name and password passes into the organization's systems through a security portal or through a Virtual Private Network (VPN), the results are the same—the user (or machine that hacked into the system) usually gets full access to the organization's systems. Adequate controls inside the system can limit the areas and types of access provided, but this may not be adequately implemented in many organizations.

It gets worse—a phishing email can trick a user into giving up his or her credentials by presenting a link to a well-crafted site designed to collect credentials. Clicking on an application may open key loggers that harvest user credentials or log keystrokes (and capture potentially valuable information from the user by monitoring every keystroke) or create exposure to other attacks. Data breaches can be accidental—as in these examples—or on rare occasions can be the direct work of a person inside the company.

There's also a basic problem with passwords—they often aren't secure because they're commonly reused. The password used by an employee to gain access to the corporate network may be the same password that's used to unlock the user's home computer, or to log into a personal mail server. Passwords may be updated infrequently, or even stored in an unencrypted file that shows the user names and passwords.

MULTIFACTOR AUTHENTICATION

A higher degree of security for connecting users and applications is provided by two-factor authentication (2FA) and multifactor authentication (MFA). These take security a step further by requiring verification of two (or more) of the following:

- **SOMETHING YOU KNOW:** a password, PIN number, unique information or other type of unique knowledge.
- **SOMETHING YOU HAVE:** a hardware key embedded into the phone or computer, a USB device or dongle that provides a unique code or other public key interface (PKI) data, or a Transport Layer Security (TLS) certificate—unique to the user's computer, phone or other device—that identifies the user to the system being accessed.
- **SOMETHING YOU ARE:** for instance, a biometric (fingerprint or retina scan are frequent identifiers).

"I log in," says Andy Ellis, Akamai's chief security officer. "I use a TLS certificate—there's a different one on every one of my devices, so the system knows which device has connected. I then get a push that verifies that I'm also holding my phone—or even better, my watch. If my watch is on, it'll just ping my watch and say, hey, is that really you logging in?"

Indiana University applies 2FA and MFA a bit differently. Dan Calarco, chief of staff for the vice president for information technology at the university, says that the organization uses 15-character passwords as one part of its 2FA efforts. "We've ended password expiration," says Calarco. Because people are using long passwords, "we have found that password reuse is not an issue for us, and so when combined with a second factor, we do not need to expire passphrases." Calarco notes that the university requires two-factor authentication. It uses a third-party app, SMS, voice calls and tokens as second factors for authentication and biometrics (fingerprints, face ID) as third factors.

He describes the use of a personal cell phone as three-factor authentication: "They need to use a fingerprint [who they are], to get into the phone [what they've got] and use password authentication [what they know]." The university carefully controls which areas users can access, ensuring, for example, that a student can't access human resources data.

"It's unlikely that passwords will be going away in any short timeframe," says Doug Barth, coauthor of the book *Zero Trust Networks! Building Secure Systems in Untrusted Networks.* Barth believes that the use of devices with secure private keys—like cell phones, USB devices with unique keys, or, perhaps, a smart watch like that of Akamai's Ellis—"in combination with passwords" makes credential theft "far more difficult."

The use of multifactor identification is a basic step towards rebuffing attacks, but **a truly effective defense requires a conceptual shift away from security at the network layer to security at the application layer. Enterprises must move from trusting the person who logs in—whether by password alone or multifactor authentication—to an approach known as zero trust.**

> "It's unlikely that passwords will be going away in any short timeframe."
>
> **DOUG BARTH**
> COAUTHOR, *ZERO TRUST NETWORKS! BUILDING SECURE SYSTEMS IN UNTRUSTED NETWORKS*

INTRODUCING ZERO TRUST

Zero trust plays off the idea that it's no longer safe to assume that any device or employee anywhere, whether on an internal network or in the cloud, is trustworthy. It's not saying that all employees—or perhaps that any employees—are not worthy of trust. Rather, it acknowledges that it's possible for employees to become victims of phishing attacks, click on malicious websites or perform other "innocent" acts that expose the organization to attacks. It also acknowledges the low risk of "bad actors" inside organizations, and actively controls their access to organization resources.

Zero trust recognizes that risk is everywhere. No asset—neither the user nor the application—can be considered trustworthy, and no connection is established until both parties in the communication validate each other. This goes beyond just multifactor authentication—not only is the user challenged by the application, but the application is also validated by the user. This is done through exchange of keys and encryption at both ends of the communication.

In zero trust, control shifts from the network layer to the application layer. A user who has been validated is allowed access only to the applications and data that the user is authorized for.

In contrast to systems that provide access to multiple applications and data sources once a user has been able to log in and get past the perimeter, zero trust systems provide access based on a database describing the applications, authorized users and conditions of use, such as days and times.

For example, Akamai offers what it calls Enterprise Application Access (EAA), a product that controls application access by users. It validates the users based on a proxy created after a user and device are authenticated. A database in EAA controls access to applications, databases and other company digital assets. A wide range of factors can be applied, including day of week, time of day, type of application, data that can be received or input, and multiple other factors.

"Broadly speaking, authenticating the user of a device [is done] before making connections further into the network, in contrast to companies with a VPN. The VPN says that 'if you can access a VPN, you can access [system resources],'" says Barth. He notes that "the VPN case only authorizes users at the session level, which can last for days, versus the zero trust, which authorizes at the request level—meaning that every action is authorized."

SECURITY AT THE EDGE

User validation and creation of a proxy are best performed near the edge, in physical locations that are near to the laptop, smartphone or other device that is logging in. Zero trust is the how, a superior way to authenticate. Edge is the where, the best place for authentication to happen.

"When you think about application development behind the proxy, you want to validate the users near the place that you site them. The proxy identifies them, and developers can upload specific authorization rules. There's a nice degree of separation between the application needing protection and who is doing the authentication for them," Barth advises.

Processing at the edge is one of the key factors that improve zero trust performance. The ability to process authentication and to validate data moving between the user's device and a central server—or another device on the internet that is close to the user—both relieves the more centralized server

> If you can't explain your security model in words that a non-IT or non-security executive can understand, then your model is too complex to survive the real world."
>
> **ANDY ELLIS**
> CHIEF SECURITY OFFICER, AKAMAI

from handling authentication and improves the speed of interactions with the user.

Zero trust authenticates all users and inspects all traffic. This is especially important as a first defense against malware and malicious applications that may otherwise reach a user. A zero trust system should be able to detect bots and make application access decisions that shield the user from accessing malicious content. The user may not know that the threats are intercepted, but the results—fewer security incidents and reduced business disruption—will be apparent to those responsible for company or agency security.

With zero trust and two-factor or multifactor authentication, single sign-on (SSA) may be possible, enabling access to web and company assets without requiring passwords. For users—especially those who have to enter long strings of letters, numbers and special characters onto a phone's tiny screen—the use of single sign-on on a zero trust system is a welcome relief.

One of the key strengths of zero trust is the simplicity of its underlying concepts. "If you can't explain your security model in words that a non-IT or non-security executive can understand, then your model is too complex to survive the real world," Akamai's Ellis says. He describes zero trust in simple words: "Take your applications, put them on the internet, but put them on the internet in a way that proxies into them, that ensures that every request that comes in is strongly authenticated, that we know who the users are, so the applications can do application-level authorization."

Akamai has developed additional products and services that enable zero trust. Its network of more than 240,000 edge devices can perform authentication, application access control and other processes in support of zero trust. For information about a variety of approaches to zero trust, Akamai has posted a series of articles that provide a look at each major approach.

CONCLUSION

Reports of data breaches at large organizations are probably the tip of the iceberg. Organizations of all sizes are vulnerable to attack if they rely on perimeter controls and don't evaluate and validate every user and every application access. Zero trust is a new approach that reduces many of the risks that are associated with reliance on network layer security by putting security at the application layer. At the application layer, systems can provide more effective controls over access to enterprise resources and data.

Zero trust is being adopted by an increasing number of organizations, both large and small. It's not a specific set of hardware or software products or a fixed architecture—rather, it's an approach to security that organizations must seriously explore.

Although it's axiomatic to believe that security will never be attack-proof, the adoption of zero trust—including strong application-level controls and increasingly secure authentication methods such as multifactor authentication—is beefing up the security of enterprises.