Cybersecurity:
A Moving Target

Security threats continue to change, and the threat perimeter continues to evolve. Agencies must find a way to keep up, both in their approach and technologies, because when it comes to securing data, applications, and networks, the federal government has work to do.

According to one Senate report, many agencies today still rely on outdated and insecure systems, haven't applied all required security patches, and have not paid attention to all threats and weaknesses. "Hackers with malicious intent can and do attack federal government cyber infrastructure consistently," said Sen. Rob Portman, R-Ohio, chairman of the investigations subcommittee in a statement released with the report.

To address these pressing issues, President Trump in 2017 issued Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. The order outlines steps agencies should take to modernize IT infrastructure and work with partners to more fully secure critical infrastructure.

But it's not that simple. Federal agencies tend to have higher volumes of attacks, simply because of the vast attack surface. In addition, government organizations tend to be more of a target than those in other sectors. There are numerous examples, such as the data filtration attack on an Office of Personnel Management (OPM) database several years ago affected more than 21 million citizens.

In addition to scale, agencies often require a higher level of reliability and service. What's more, the government has something of a least common denominator problem. As Shawn McCarthy, a research director at IDC Government Insights, puts it: "If you are in industry, you can require everybody you deal with to use a specific piece of software and specific types of security. But the government has to 'blend down' to ensure that everyone interacting with government systems can interact successfully. That will inevitably lead to more security vulnerabilities."

And like all other organizations, federal agencies are quickly moving toward an essentially perimeter-less world. More workloads than ever are in the cloud, often accessed by users working on their own personal devices. Those devices are notoriously less secure than agencies would demand of their own resources. In addition, a growing number of sensor-based devices, which have their own security weaknesses, are being added to agencies every day.

HOW GOVERNMENT AGENCIES CAN KEEP PACE

With data now being one of the most valuable commodities, it's more important than ever to use proven methodologies, processes, and frameworks to make sense of it, apply metadata, and manage it. That's only possible with a solid data-driven architecture.

With that in mind, there are several steps agencies can take to improve cybersecurity.

One of the most important is implementing the concept of Zero Trust. While Zero Trust is not a technology, it is an important concept that includes critical cyber-protection capabilities. Though the specific tools and functions agencies can use to achieve Zero Trust can vary, IDC defines it as having three important capabilities: software-defined perimeters, micro segmentation, and identity-aware proxies. A software-defined perimeter is essentially a next-generation VPN, while micro segmentation provides more granular access control inside a data center. Organizations use identity-aware proxies to control access to resources in the cloud via authentication and user-based access control.

More organizations than ever are taking this advice. According to one recent report, 72 percent of organizations plan to implement Zero Trust capabilities this year to help address cyber risks.

Throughout government, Zero Trust is having a moment too. The American Council for Technology-Industry Advisory Council (ACT-AIC) notes in a report that Zero Trust "has the potential to substantially change and improve agencies' abilities to protect their systems and data." The report goes on to explain that Zero Trust satisfies many of today's cybersecurity issues because it shifts from the traditional security policy of all assets in an organization being open and accessible to requiring continuous authentication and authorization for any asset to be accessible.

The federal government itself is also on board. The National Institute of Standards and Technology (NIST) released the second draft of its Zero Trust Architecture in February. It details the core logical components that make up a Zero Trust architecture network strategy.

LEVERAGING INSIGHTS FROM DATA

Despite these constraints, agencies must find a way to keep pace with the changing cybersecurity landscape. But how? Resist the temptation to buy and install as many cybersecurity defense products as possible, experts say. It's also much better to keep the focus on data as a strategic asset, which is one of the key tenets of the Federal Data Strategy.

Leveraging data helps mitigate cyber risks is by employing advanced analytics, artificial intelligence, and machine learning techniques. By analyzing data, especially with the help of artificial intelligence and/or machine learning, agencies can better predict and prevent events, enhance decision-making, and dramatically reduce the time it takes to not only detect when breaches are occurring, but predict when and how they will occur.

It's about raising our level of analysis to consider entities: people, computers, emails, and their relationships, rather than trying to assemble the full picture one verbose log line at a time," explains Olya Flores, Director of Data Transformation at Leidos. "If we are able to detect large-scale patterns across time and sources, then we are much more effective against advanced persistent threats."

One issue is that maintaining visibility has become more difficult in all environments as endpoints, from desktops and laptops to tablets and smartphones, can connect to workloads in the cloud from virtually anywhere. That makes it more critical than ever to understand exactly what is connecting to your network at all times. And that requires collecting data from every device across the enterprise, such as what processes are running and who is logged on. With that information, it is much easier to spot anomalies.

"The goal is extracting information about things that seem out of the ordinary without extracting too much," says Sean Black, director of cybersecurity at Leidos. "If you took every input, especially in the cloud, it would produce too much data, which would be hard to manage and very expensive. So you have to figure out what's valuable."

Leidos has put these concepts into practice for its federal customers. For example, Leidos is currently supporting DISA's Global Information Grid Services Management Operation (GSM-O) program to modernize DoD communications and networks. In the area of cybersecurity, the contract has succeeded in spearheading the implementation of one of the world's largest security gateways, the Joint Regional Security Stack (JRSS). With JRSS, Leidos supported selection of best-0f-breed tools that provide mitigation, detection and network monitoring capabilities to support a variety of cybersecurity use cases.

Leidos has also helped consolidate operations center support from around the globe into a single, virtual network operations center. Still to come is consolidation of hundreds of network security services and stacks that the DoD maintains at each of the local base, camp, and post station networks into one of up to 48 regional security stacks.

Getting ready for the next generation of threats

Protecting your agency's assets is difficult, and it's only going to get worse. According to IDC, the number of 5G wireless connections to networks will rise to more than one billion by 2023, compared to 10 million in 2019. And there will be 125 billion Internet of Things (IoT) devices by 2030.

There are good reasons why these technologies are growing so fast. 5G promises much faster speeds and lower latency than 4G, and carriers are making real progress in getting the infrastructure in place. Internet-connected devices, commonly called IoT, provide critical information to their users and organizations. In the business world, they are becoming commonplace in healthcare systems, vehicle communications and transport, digital control systems, surveillance, wearable biometrics for combat, and all types of appliances and fixtures.

While the benefits are undeniable, so are the risks. Because 5G is so efficient, employees are likely to use it on their own devices instead of connecting to the agency's WiFi or connecting via Bluetooth. Employees also may use 5G for their IoT sensors. While neither 5G or IoT sensors are inherently insecure, the explosion of use for these technologies may make it difficult to control. If agencies aren't aware of all devices connecting to the 5G network or what they are accessing, how can they protect those devices and their agency's data?

The solution may be artificial intelligence. With the right AI tools and applications in place, agencies will be able to more easily and quickly determine what's normal and what may be an anomaly.

And then there is the unknown.

"This stuff is still pretty new," says Pete Lindstrom, a vice president for security at IDC. "I don't think all of the vulnerabilities have been discovered yet."

GETTING IT RIGHT

Clearly, keeping up with changing security threats and technologies isn't easy. The best way to get a handle on it, Flores says, is to make sure that you use repeatable processes, along with frameworks and methodologies that allow your agency to pivot to new technologies and approaches when necessary.

"At Leidos, we have established proven frameworks for many areas, including agile, CI/CD, cloud migration and security and cyber workflows, to list just a few," she explains.

Making sure your architecture is as open as possible also is important. Without that, agencies can end up with solutions that aren't a good fit. That results in extra time and expense to build something around that solution or buy new tools. By establishing an interface-oriented data pipeline, you can create the foundational service utility-level infrastructure that ensures that data flow can be used by any tool, and yet data remains fully controlled and governed by the pipeline itself, she added.

To ensure that these methodologies and frameworks work well, Leidos has been known to experiment on itself. As new concepts are developed, the team applies them first in the Leidos environment. "We have made ourselves be a proving ground for those cutting-edge technologies but with our federal agency customers in mind. We focus on how to extract the most value for the people we serve without introducing unnecessary risk," Flores says.