GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

Author: Green, John

Title: "Why the Network Is Central to IoT Security"

Website: Dark Reading Endpoint

Organization: Dark Reading

Date: 31 July 2019

URL: https://www.darkreading.com/endpoint/why-the-network-is-central-to-iot-security/a/d-id/1335367

Accessed: 19 Oct 2019

Synopsis: Is there something strange about your network activity? Better make sure all of your IoT devices are under control.

In a large school district, there was a digital sign for a snack area that no one had thought about for months. Eventually, the snack area was removed, yet the sign was still plugged into the district's network. For months, it turns out, the sign had been compromised by attackers and was communicating with 100 different countries.

The case highlights the problematic nature of the Internet of Things (IoT) and the ingenious ways bad actors are taking advantage of the fast-growing attack surface created by IoT. It also shows that security must adapt to this new reality if enterprise networks and sensitive data are to remain protected.

Why the Network Is Central to IoT Security

Jon GreenCommentary

Is there something strange about your network activity? Better make sure all of your IoT devices are under control.

In a large school district, there was a digital sign for a snack area that no one had thought about for months. Eventually, the snack area was removed, yet the sign was still plugged into the district's network. For months, it turns out, the sign had been compromised by attackers and was communicating with 100 different countries.

The case highlights the problematic nature of the Internet of Things (IoT) and the ingenious ways bad actors are taking advantage of the fast-growing attack surface created by IoT. It also shows that security must adapt to this new reality if enterprise networks and sensitive data are to remain protected.

The challenge around IoT security will only grow. Worldwide spending on IoT is expected to hit $745 billion this year and blow past $1 trillion in 2022. For enterprises deploying IoT devices, security remains the top technical issue as those looking to compromise the devices are often sophisticated nation-states or organized crime organizations.

The myriad IoT devices come with an almost equal number of challenges:

- There is a wide variety of innate security within them. Some are intended for enterprises while others are consumer-focused, but both types tend to come with much less in terms of security testing than a laptop, an iPad, or other device that might be purchased by an IT department.
- They're not well-monitored, as was the case with the fish tank. As long as the devices are working with reasonable performance, most enterprises won't notice if something goes wrong, as opposed to a laptop that has antivirus protection and other ways to detect attacks.
- In enterprise environments, people connect these devices without always involving anyone from IT. They see an open port and connect a device into it. As a result, enterprises often don't know everything that's on their networks.

There is a lack of visibility and security into the devices in what is an increasingly distributed enterprise IT environment. Often the devices are deployed on the interior of the network, and while some may be talking externally to a public cloud or other Internet-based systems, many communicate internally to other systems on the network.

Security deployed at the network's perimeter will be blind to such communications unless the enterprise is watching the internal network, which many aren't. If those devices are compromised, they become a launching pad into other parts of the network. The school district's digital sign is proof-positive here.

The network is now the focal point for IoT security. The devices connect into the network, the network touches all data and workloads, and this is how hackers can

move laterally to compromise whatever systems and data are on the network. Through the network, users and devices can be authenticated, policies and rules put in place to control access and behavior, and visibility can be increased to detect anomalies.

The top IoT issue is that you shouldn't rely on physical security to keep things off a network. There are many places in the wired network that are wide open and there is little network access control. There's more control and authentication on the wireless side, but even there, devices that are authenticated often get dropped into an internal VLAN and from there are uncontrolled.

Key steps that can be taken to better protect an enterprise network:

1. **Outlaw anonymous connections.** Enterprises must know *every* device that is connected, whether a laptop or a sprinkler controller.
2. **Determine what the "thing" should be allowed to do on the network.** IoT devices are static in nature; they do the same thing repeatedly and talk only a single protocol or two. Determine what "good" looks like for these devices.
3. **Use the network to enforce those rules.** Many people don't take this last step, but without enforcement, polices mean little. If the cameras need to talk only to the network DVR, then use the network to allow only that behavior.
4. **Monitor for abnormal behavior.** If an enterprise sees a device operating outside of what's normal, something is probably wrong. Fortunately, because you followed step 1, you know what's on the network, so tracking down a misbehaving device should be easy.

Central to the issue of IoT security moving forward is the growing need for security and networking folks to communicate. Getting this to happen is sometimes easier said than done. In some ways, the two groups are often adversarial. Network operators are happy if all the network packets are flowing quickly with high availability and low latency — even if all those packets are carrying malicious traffic. The security group would probably be happiest if nothing flowed through the network at all.

The network plays a critical role in two areas: detecting when an attack is taking place and responding to the attack by shutting down the device, limiting it, or slowing it down. There is much you can do with the network infrastructure. People will look to firewalls for solving network security problems, but don't tend to use a firewall for every single switch port. The security capabilities must be built into the network itself.

That will mean cooperation between network and security groups. Because this is a cultural issue, it will need to start with high-level executives. That doesn't necessarily mean both sides will report into the same structure. However, the security pros will have to determine what needs to be protected and the network folks will have to decide how to make it happen, all the way at the network edge where the devices connect.

Bringing these two groups together will be a challenge, but it's necessary. Without it, there will be more data breaches coming from a wider variety of things rather than end-user systems. HVAC controllers, TV screens, smart fish tanks, and other IoT devices will continue to be used by hackers seeking ways into critical parts of the network. And the IoT devices won't be getting better from a security perspective

anytime soon because many of the makers of these things aren't focusing on that.

Related Content:

- **The State of IT Operations and Cybersecurity Operations**
- **7 Malware Families Ready to Ruin Your IoT's Day**
- **Focusing on Endpoints: 5 Steps to Fight Cybercrime**
- **Insecure Home IoT Devices a Clear and Present Danger to Corporate Security**

Jon Green is responsible for providing technology guidance and leadership for all security solutions, including authentication and network access control, UEBA, encryption, firewall, and VPN. He also manages Aruba's Product Security Incident Response Team (PSIRT) and Aruba ... View Full Bio

More Insights