Domotz Case Study

CyberPrivacy: Using Domotz to keep Clients aware

October 2020

domotz

Managed Service Providers (MSP) are being forced to think about how to protect their clients digital assets. Security has moved away from the simple lock and key to the digital domain. Ransomware demands have exceeded a billion dollars in the United States alone and the costs associated with repairs are nearly ten times that amount. In this Case Study, we will address how one MSP has leveraged Domotz to protect his clients.

A Market in the making...

CyberPrivacy is a security company which actively deploys, monitors, and maintains home and business networks to reduce the user's digital footprint and provide a segmented cybersecurity approach. Based in an amazing historical building in Pueblo, Colorado, the team at CyberPrivacy is focused on ensuring their clients have a reduced cyber footprint and fewer attack surfaces. Their vision is to maintain an appropriate balance between the technology and convenience needs of the client, while ensuring a healthy online privacy profile.

A Holistic Approach...

Next generation firewalls, managed switches, and secured enterprise-grade wireless access points are just the beginning of how CyberPrivacy protects their clients. A prescribed set of processes are established with the client to meet the balance necessary between convenience and the companies needs. Furthermore, the CyberPrivacy team's certified ethical hackers constantly review their clients networks, systems and services to ensure the created processes are in place.

Implementation is what matters...

While network zoning and secure internet access may seem standard, the CyberPrivacy team takes it further…way further. Based on the client's needs, they focus on individual identity protection, including geo-tracking protection. Think of this bodyguard services at a digital level. For the client, setting up a segmented network is not enough, they look at how each network is actively behaving and where devices on those network segments are going. Any device that reaches out to what is considered a compromised site is abruptly quarantined and promptly managed.

Scaling these processes...

CyberPrivacy implements Domotz's service on every one of their client's networks. Domotz monitors each VLAN and subnet that has been segmented

domotz

for the client.   The CyberPrivacy team realized quickly that awareness of new devices on the network is critical to stopping abnormal behavior before it even starts. Leveraging Domotz's new device discovery alerting, tickets are automatically created and prioritized based on the client's needs.   In addition, Cyberprivacy takes advantage of Domotz's Network Security Scanner functionality which looks for open ports on the WAN and LAN side of the router/firewall. These two services from Domotz has become a valuable assurance tool by automating these fundamental checks, allowing their team to focus on more advanced and critical client needs.

Assessments as a Service...

The first non-intrusive assessment step with any new client is to deploy a Domotz agent and perform a security status scan. For a quick assessment with a new customer, this is one of the more cost-effective approaches. Within 24 hours the Domotz agent reports any potential port vulnerabilities. In many cases, Domotz has returned results that the client was not even aware of. Based on the assessment report from Domotz, CyberPrivacy is able to quickly demonstrate and educate the customer with the next necessary security steps, ultimately leading to new services employed by the team.

Critical need for Reporting...

Continuous reporting on activities is a must do for CyberPrivacy. Clients must be made aware of the services they are receiving, and the support team leverages detailed information provided by Domotz to update their customize reports.   While the CyberPrivacy accesses their client's network through Domotz's secure connectivity solutions, they use the logging features to include how often accesses are made.

All things considered...

While CyberPrivacy goes above and beyond for their clients, it is important for MSPs to see how they leveraged Domotz to get better scale on what would normally be considered a rather tedious, but necessary task. MSPs should be looking at secondary checks to vulnerabilities on the networks they monitor. They should also be taking advantage of the logging and reporting features, including the network topology mapping to bring awareness to their clients.

For more information about Domotz

Website:	https://www.domotz.com
Email:	sales@domotz.com

For more information about CyberPrivacy

Website:	https://cyberprivacy.today
Phone:	1-801-658-0051
Email:	info@cyberprivacy.today