ENHANCED CYBERSECURITY SERVICES (ECS) PROVIDE AN EXTRA LAYER OF PROTECTION

CenturyLink offers a new tool in the fight against cyber attacks

Intensified media attention and public outcry around recent data breaches have heightened public awareness of the real impacts and costs of inadequate IT protection, making many organizations question their own networks' immunity and unknown vulnerabilities. And while people tend to blame the perpetrators for other criminal acts, the invisibility of cybercriminals can cause people to blame the victims for having ineffective cyber protections.

MITIGATING GOVERNMENT-TARGETED THREATS

One of the most insidious of all cyber infections is something called a "bot" that can execute tasks on behalf of cybercriminals whenever they want. Despite having security protocols in place, a bot can gain entrance to an organization's network by hitching a ride on a link or email attachment and then sit undetected on a computer for minutes, months or even years. Once activated, a bot can reach out from a command-and-control master location and allow criminals immediate entry into an organization's internal network.

Unfortunately, government organizations are not immune to this sort of cybercrime and repairing cyber damage can be a time consuming and very expensive process. Even cyber intrusions that aren't highly sophisticated can take up to 120 days to detect. And once threats have been embedded on a network, the cost to mediate them can add up to millions of dollars.

CenturyLink, the country's third-largest telecommunications company and a leading network provider, is helping spearhead the fight against cyber intrusions into the IT systems of government agencies and enterprise organizations. CenturyLink's extensive work in the cybersecurity space has led it to form a valuable relationship with a powerful ally in the nation's struggle against cybercrime: the U.S. Department of Homeland Security (DHS).

PRESIDENTIAL MANDATE: PROTECT CRITICAL INFRASTRUCTURE

DHS has a presidentially mandated mission to protect critical infrastructure sectors that, should they be negatively impacted, could threaten national security and prevent our government and citizens from conducting normal business.

Those 16 critical sectors include the broad building blocks of our nation's infrastructure and economy, such as state and local governments, the defense industrial base, energy, healthcare, communications, financial services, food and water, and transportation sectors. You can see the federal government's full list at www.dhs.gov/critical-infrastructure-sectors.

CenturyLink is one of only two commercial service providers authorized by DHS under an innovative public-private partnership to provide Enhanced Cybersecurity Services (ECS) to organizations within

these critical infrastructure sectors. The ECS program's mission is to enhance the sharing of sensitive, government-furnished information with ECS providers and participants to help protect America's critical infrastructure sectors from advanced cyber threats. ECS is one of the federal government's weapons of choice in America's battle against cyber attacks.

As an original provider under the 2010 pilot program that became ECS, CenturyLink has been involved from the start, which gives it the industry's highest level of ECS technical and operational expertise. Through its long-standing relationship with DHS, CenturyLink is able to provide ECS customers with exclusive security information and powerful protections that are unavailable in the standard commercial marketplace.

"Part of the underlying requirement that allows us to operate in this space is our security infrastructure," says CenturyLink Government's Senior Vice President and General Manager Diana Gowen. "DHS knows it can trust us with sensitive ECS information and that it will be handled appropriately when inserted into our service offerings for customers."

HOW IT WORKS – THE ECS ADVANTAGE

The path from threat indicator to threat eradication begins with DHS, which works with agencies across the federal government to gather a broad range of sensitive cyber threat information. On a frequent basis and during sudden emergency windows of action, DHS supplies those detailed threat indicators to CenturyLink, which integrates that data with its own threat indicators into the ECS operational system.

Through the use of threat indicators, CenturyLink provides ECS customers with network-based inbound email filtering that neutralizes dangerous email strings or attachments, notifies network administrators and prevents harmful code from becoming embedded into an organization's IT infrastructure. The company also provides ECS customers with Domain Name System (DNS) protection and notifications, which prevents users from accessing malicious DNS sites and provides protection from infected machines establishing command-and-control links to external entities.

Protecting critical infrastructure against evolving cyber threats requires a layered, dynamic approach – one that evolves to confront new technologies and threats. ECS isn't a silver bullet that deflects all cyber hazards, but it is an enhancement that is meant to work in tandem with the standard security protocols agencies should already have in place. "Organizations should do everything to protect every security layer," says Gowen. "This exclusive content from DHS enables us to see things others can't, to defend against things that others are unaware of and to provide specific protections that can't be delivered any other way."

Is Your Agency Vulnerable?

Certain government sectors maintain data files of particular interest to cybercriminals who share, buy and sell blocks of this personal data internationally. This can take the form of a mosaic effect, whereby small bits of seemingly innocuous data are pieced together from different sources to tell a bigger story.

Government agencies should consider whether they have adequate security protections in place for these types of data, which include public records from:

- Departments of motor vehicles
- Franchise tax boards
- Departments of veterans affairs
- State medical facilities
- Departments of public health
- Mental health services
- Departments of correction
- Divisions of human resources and employee benefits
- Public employee retirement divisions
- Social services divisions
- Public K-12 schools and universities

TRANSCENDING STANDARD SECURITY

CenturyLink has a full complement of augmented cybersecurity services for a well-rounded security posture, as well as a broad array of ECS engineers, software programmers, threat analysts, subject matter experts and trainers. This formidable partnership between CenturyLink and DHS provides state and local government ECS customers with 24/7, state-of-the-art defenses against network intrusions and cyber attacks.

Gowen says, "Given the ever-growing sophistication of malware and criminal operators, now is a smart time to reach out to us for a conversation on the sensitive records your agency needs to protect."

Learn how CenturyLink ECS can complement your existing security portfolios to protect against cybercriminal activity in the government environment – and protect the constituents who count on you for safety – at www.centurylink.com/gov or email the CenturyLink ECS team at ecs@centurylink.com.

centurylink.com/link

Data • Voice • Cloud • Managed Services

CenturyLink® Government