How Government is Facing Cyber Security Challenges

The U.S. government will spend almost $15B on cybersecurity in 2019[1], because government is one of the top 5 industries most targeted by cyber espionage today[2].

As holders of a wealth of confidential information for millions of users, top-notch cybersecurity for government agencies is critical.

The Best Offense is to Build a Better Defense

If you want to combat threats, you need to first know what they are. Here are some of the top cyber threats and how CenturyLink offers solutions to help you mitigate them.

1 Denial of Service and Botnets

We respond to and mitigate approx **120** DDOS ATTACKS PER DAY[3]

Botnets (or zombie systems) are millions of systems infected with malware that attack a target by overwhelming bandwidth and processing capabilities.

DDoS services deployed on-site or in your data center can help to eliminate attack traffic before it reaches your websites—while legitimate traffic continues without interruption.

2 Man-in-the-Middle and Session Hijacking

These attacks occur when a hacker inserts itself between the communications of a client and a server through IP spoofing, session hijacking and replay.

CenturyLink's actionable threat intelligence utilizes government-furnished threat and technical information through **CenturyLink's Intrusion Prevention Security Service program with DHS for federal agencies.**

3 Malware and Ransomware

Attackers send malware (short for malicious software) that gets installed in your system without consent. It often attaches itself to legitimate code, then lurks in applications to replicate itself to other systems. Ransomware is a type of malware designed to block access to a computer system until a sum of money is paid.

49% of agencies can detect and whitelist software running on their systems[4]. CenturyLink is a top ranked managed security service provider that uses both network and premise-based solutions to secure agency boundaries with proven firewall, anti-virus, anti-malware, intrusion detection, intrusion prevention, vulnerability scanning and incident response services.

4 Spear Phishing

Spear phishing is an attack that combines social engineering and technical trickery to extract personal information from a victim. Most commonly, it occurs by way of an email that appears to come from a trusted source that influences users to compromise their security without even realizing it.

The average user receives **16 malicious spam emails per month[5].**

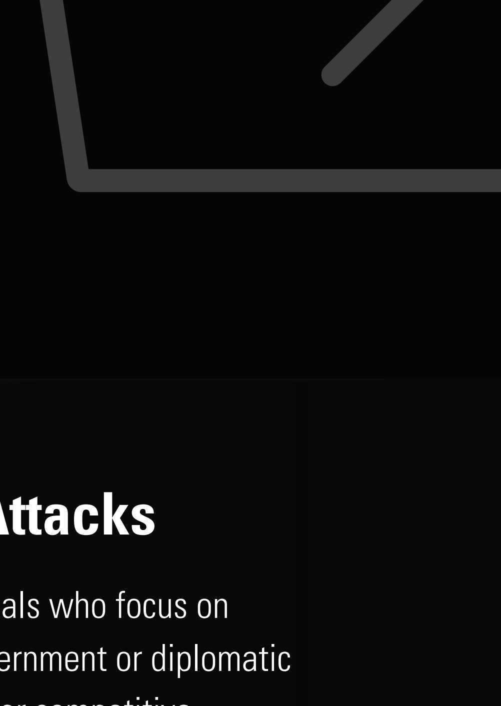
5 Password and Cracking Attacks

Pretty simple: passwords authenticate you to access systems. If hackers have your password, they have access to your systems. Hackers can "sniff out" unencrypted passwords, break into a password database or use software that guesses commonly used passwords.

Federal agencies are adopting multi-factor authentication Personal Identity Verification cards for increased accountability and control. **Agencies now enforce card control among 93% of users who have access to sensitive data[6].**

6 Data Exfiltration, Theft and Fraud

Data exfiltration is the unauthorized copying, transfer or retrieval of data from a system through a portable media device or a remotely controlled application.



Only 27% of agencies report the ability to detect and investigate attempts to access large volumes of data[7]. Even fewer report testing these capabilities annually. Simply put, most agencies cannot detect when large amounts of information leave their networks.

7 Nation-State Attacks

State-backed cybercriminals who focus on hacking into military, government or diplomatic systems to acquire data for competitive intelligence, influencing politics, conducting warfare and other state-sponsored cybercrime is a real problem.

Hacking by foreign governments was a prominent issue during the **2016 U.S. presidential election[8].**

What Are Agencies Doing to Prepare?

Agencies are partnering with top managed security service providers like CenturyLink to create cybersecurity solutions that help agencies prevent, respond and remediate cyber attacks protecting and defending the integrity of their mission and data.

71 of 96 federal agencies rely on cybersecurity programs deemed "at risk" or "at high risk."[9]

Where to Go for Help?

CenturyLink has multi-threat, multi-layered security offerings, highly skilled security experts, best-in-breed government contracts and cybersecurity standards compliance.

Learn more at our Federal Government page.

References

1: Statista, Global Industries Most Targeted by Cyber Espionage, 2017
2: Statista, U.S. Federal Government IT Expenditures, 2011-2019
3: CenturyLink, Threat Research Labs Report, Full Year 2017
4: Office of Management and Budget, Federal Cybersecurity Risk and Determination Report, May 2018
5: Symantec, Internet Security Threat Report, Volume 23
6: Office of Management and Budget, Federal Cybersecurity Risk and Determination Report, May 2018
7: Office of Management and Budget, Federal Cybersecurity Risk and Determination Report, May 2018
8: Statista, 2016 Election Stats and Facts on the Vote, 2017
9: Office of Management and Budget, Federal Cybersecurity Risk and Determination Report, May 2018