PUBLIC SECTOR:

COMBATTING MASSIVE CYBER THREATS

Executive Summary

The public sector has become a favored target for cyber criminals. Armed with automated botnets, hackers rummage through computer systems to locate under-secured "soft targets." In recent years, U.S. state and local government agencies have fallen prey to cyber attacks. Legacy security is proving ineffective against the growing legion of diverse, sophisticated, and confrontational cyber threats.

What's shocking is that 29% of internet traffic is believed to consist of malicious bots.[1]

Public agencies collect and store sensitive data. Like the private sector, government institutions have gone digital. The addition of cloud, mobile, and SaaS have expanded an organization's attack surface. It further illuminates the fact that your cyber security is only as strong as your weakest point.

In this whitepaper, we'll discuss the two main cyber threats that public sector organizations face: ransomware and data breaches. We'll then recommend foundational practices that can help bolster your cyber security.

[1] "The Internet is Mostly Bots," by Adrienne LaFrance, The Atlantic, January 31, 2017.

Public Sector Threat Landscape: Two Sides of a Tarnished Bitcoin

Ransomware

Ransomware is malware that infiltrates networks to freeze access to computer systems, and paralyze functionality until a ransom is paid, usually in Bitcoin cryptocurrency. However, dishing out coins is no guarantee that cyber criminals will restore your access to data, networks, or computers. Research carried out by CyberEdge Group shows that less than half of those who opted to pay the ransom were able to recover their files.[2]

Targeted ransomware attacks have been on the rise. In the U.S., more than 163 ransomware attacks targeted local and county governments in 2019, a 196% increase over the previous year.[3] In Europe, the EU warned that ransomware remains the top cybercrime threat, with governments being particularly vulnerable to such attacks.[4] Furthermore, government agencies are particularly vulnerable because of the expanding attack surface, their use of outdated technology, and limited budgets.[5]

In the U.S., the FBI has issued a "High-Impact" cyber attack warning to businesses and organizations, citing the ongoing criticality of cyber threats.[6] Losses from ransomware are on the rise as hackers are launching attacks that are more targeted, sophisticated, and costly.[7]

> "At least three U.S. States will declare states of emergency due to waves of ransomware in 2020. Ransomware, which carried a price tag of over $10 billion this year in attacks, will continue to plague state and municipal agencies lacking appropriate skills, controls, and ransomware countermeasures."[8]
>
> *— Jon Oltsik, Senior Principal Analyst and Fellow, Enterprise Strategy Group (ESG)*

StateScoop developed the interactive Ransomware Attacks Map, documenting 260 known public sector ransomware attacks in the U.S. since 2013.[9] The authors noted the alarming increase in ransomware attacks over the last several years, with new high-profile incidents occurring every few weeks.

---

[2] "Ransomware: To Pay Or Not To Pay, That Is Still A Real Question, October 9, 2018.

[3] "Ransomware Increasingly Targeting Small Governments," by Robert Lemos, Dark Reading, March 11, 2020.

[4] "European Union Finds Ransomware Is Top Cybercrime, VOA News, October 9, 2019.

[5] "Ransoming Government," by Pete Renneker, Deloitte, March 11, 2020.

[6] "FBI Issues 'High-Impact Cyber Attack Warning' – What You Need to Know," by Davey Winder, Forbes, October 3, 2019.

[7] Ibid.

[8] "42 More Cybersecurity Predictions for 2020," by Gil Press, Forbes, December 12, 2019.

[9] "Ransomware Attacks Map chronicles a growing threat," by Benjamin Freed, StateScoop, October 22, 2019.

Here are a few examples of municipalities hit by ransomware in 2020[10]:

- A county in New Mexico paid a ransom of $250,000 in bitcoin to restore servers knocked offline by cyber extortionists.
- An Alabama city was hit with DoppelPaymer ransomware, shutting down the city's email system.
- An Oregon County's server, internal computer systems, website, and email networks were taken offline by a ransomware attack, forcing decision-makers to pay a $300,000 ransom.

Data Breach

The data breach is an exploit where sensitive data is stolen by hackers or is accidentally exposed in an untrusted environment. Breaches can have severe consequences on citizens when names, addresses, phone numbers, social security numbers, credit card information, and even drivers' license numbers are stolen. Personal information can be also be used for identity theft and it can take a victim years to unwind bogus accounts with creditors. Regaining trust in an ineffective government entity can take even longer.

These recent data breaches have proven that no government agency is immune from cyber theft:

- A national postal service breach exposed data involving 60 million users, allowing identity thieves to intercept package deliveries.[11]
- A government payment service leaked more than 14 million customer records, including names, addresses, phone numbers, and the last four digits of the users' credit card numbers.[12]

Using legacy cyber security puts your organization at grave risk, especially with the dangerous undertow of sophisticated, nation-state attacks.

- The breach of a national tax agency impacted 5 million citizens as their personal information and financial records were stolen.[13]

Protecting your organization's data matters more today than ever before. "The public sector had 23,399 reported incidents in 2019, with 330 confirmed instances of data being disclosed through a breach."[14] Cyber attackers work relentlessly to infiltrate your organization for financial gain or for espionage, stealing government secrets. Well-financed nation-state syndicates attack public agencies to push political or military agendas, accounting for 79% of all data breaches involving external actors.[15]

[10] "The 11 Biggest Ransomware Attacks of 2020 (So Far)," by Michael Novinson, CRN, June 30, 2020.

[11] "USPS Site Exposed Data on 60 Million Users," By Brian Krebs, Krebs On Security, November 18, 2018.

[12] "GovPayNow.com Leaks 14M+ Records," By Brian Krebs, Krebs On Security, September 18, 2018.

[13] "Bulgarian tax agency breach may have compromised 5 million people," By Mariella Moon, Engadget, July 17, 2019.

[14] "Cyber Espionage Targeting Public Sector Rose 168% in 2018," By Aaron Boyd, Nextgov, May 8, 2019.

[15] Ibid.

In addition, some insurance companies have been unwilling to pay for damages that could be construed as an "act of war" or aggression committed by a nation-state group. Despite the comfort in knowing that you have insurance, it can't be relied upon as your strongest cyber safeguard.

Government Agencies: On the Front Lines of Cyber Defense

Millions of citizens interact with their government agencies for critical needs. Citizens apply for passports, mortgages, driver licenses, social security, student loans, and other benefits. However, as we store more data online, we are also unwittingly granting more attack vectors. Thus, governments can't afford to handle this data carelessly.

A recent report called Taking the Pulse of Government Cybersecurity 2020 reveals what government cyber security professionals in the U.S., U.K., and the Middle East think of their own cyber defenses.[17] 65% of government respondents thought the pace of change was too slow in comparison to private business, and 81% believed that a slow pace of change can negatively impact national cyber defense. If government agencies can't quickly adapt their cyber security strategies, then how can they be trusted to protect the precious data of their own citizens?

For example, federal agencies in the U.S. struggle with meeting basic cyber security standards. A Senate report revealed that agencies have regularly failed to install critical security patches when notified and are using IT systems that are decades old.[17] The Department of Homeland Security still uses operating systems such as Windows XP and Windows 2003, which are no longer supported by Microsoft and are vulnerable to a slew of cyber threats.

It's not just agencies in the U.S. having trouble. Recently, 92 million Brazilian citizens were reported to have their data for sale on the dark web, and Bulgaria's tax authority was hacked, affecting five million people.[18]

What does all this mean for your organization? With government agencies facing increased cyber risks, you need a simple, scalable, and modern cyber security approach that enables a solid defense against the latest cyber threats.

For maximum protection, your organization can benefit from a multi-faceted prevention strategy, combatting threats across all attack vectors before they've unleashed malicious payloads. An easy-to-manage, unified cyber architecture focused on the prevention of (rather than just detection) fifth-generation cyber threats.

---

[16] "Taking The Pulse of Government Cyber Security 2020," by Nominet Cyber Security, June 2020.

[17] "Federal Cybersecurity: America's Data At Risk," by Rob Portman and Tom Carper, July 19, 2019.

[18] "The latest government data breaches in 2019/2020," by Stephen Pritchard, The Daily Swig, February 28, 2020.

Cyber Security for the Public Sector

Public sector agencies must maximize security across a borderless network that allows you to securely connect anyone, anywhere, anytime, and on any device. Use the following guidelines to effectively defend your organization against cyber threats:

Block Advanced Persistent Threats and Zero-Day Attacks

Implement integrated, defense-in-depth protection that enables you to detect, protect, and respond to multiple advanced attack vectors simultaneously. Leverage an integrated solution that uses antivirus, IPS protections, anti-bot, and firewall technology. Use real-time intelligence that protects against unknown malware and zero-day exploits.[19]

Continuously Monitor and Diagnose the Environment

To shed light on malicious activity, you must have full visibility and understanding over your network. The U.S. Department of Homeland Security (DHS) launched the Continuous Diagnostics and Monitoring (CDM), allowing agencies to better monitor their IT systems in real-time and address vulnerabilities instantly. The program lets you know what's occurring in a network on a continuous basis—not just at audit time. A similar program can provide your IT staff with real-time configuration monitoring against a library of security best practice diagnostics to ensure security and compliance.[20]

Secure Information on Multiple Devices

Using multiple devices has become commonplace, but this has increased the complexity of protecting sensitive data. Use integrated security that leverages a single protection architecture for mobile and endpoint-based systems such as mobile phones, laptops, and medical devices.

[19] "Security for Government Institutions," Check Point Software Technologies, August 14, 2018.

[20] Ibid.

Consolidation

Over time, many organizations have implemented stand-alone products from multiple cyber security vendors. This practice has created a "patchwork" security architecture with little or no integration between various products. The net effect is increased complexity and a lack of centralized visibility, control, threat intelligence, and management; elements required to better protect against targeted and advanced attacks. Adopting a consolidated approach can improve operational efficiency by 50% since there are fewer products to deploy and manage, and it can reduce costs by 20% since all products are under a single protection business model.[21]

Compliance

With agencies facing increased scrutiny and regulators enforcing stricter policies, your organization must adhere to higher levels of protection for citizen data. Utilize a dynamic security compliance solution that continuously monitors your security infrastructure and provides updates in real-time, ensuring that you're in compliance with the latest regulatory requirements.

User Awareness Training

Incorporate phishing simulation into your employee training programs to ensure that users can identify and avoid these cyber attacks. Even your most tech savvy people can fall prey to a well-architected phishing exploit. Social engineering scams have become so sophisticated that criminals are using artificial intelligence to fake the voice of executives and demand payment from subordinates.[22] Phishing-detection systems can help pick up subtle cues and block e-mail threats.

Conclusion

With the increases in advanced 5th generation cyber attacks that include large-scale, zero-day threats, seeking comprehensive cyber threat prevention is a top priority. As cyber attacks are showing no signs of a slowdown, your next cyber security decisions will determine how well your infrastructure and data is protected in 2020, and beyond.

[21] "Security Architecture – Check Point Infinity," Check Point Software Technologies, 2019.

[22] "Thieves are now using AI deepfakes to trick companies into sending them money," The Verge, Nick Statt, Sep 5, 2019.

A Case in Point

"With Check Point we have managed to intercept a lot of attacks. When we experienced a phishing attempt, Check Point prevented it from entering our environment and causing damage," Simone Ciotti, Network Specialist, LAZIOCrea SpA.

LAZIOCrea SpA is responsible for dealing with all IT-related activities for Italy's Lazio region. With Check Point's solutions, LAZIOCrea was able to protect the sensitive information of nearly six million residents and comply with the constantly-changing rules imposed by the government. Get the details of the case study here.

To learn how a unified security architecture can bring real-time visibility and improved threat prevention, visit the Infinity web page, or contact your Check Point representative.

For information on how Check Point meets the cyber security needs of federal agencies, visit the Federal Security page, or contact your Check Point representative.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com