RADWARE SOLUTIONS FOR GOVERNMENT

GOVERNMENT CONCERNS AND CHALLENGES

Government institutions require online applications to streamline processes, provide content and cut costs. The growth of online services and web-based content introduces new challenges to federal, state and local agencies that need to address issues like 24x7 access to critical applications to ensure end-user quality of experience (QoE) and protection of consumer records.

The public sector is targeted by an array of threat actors, from hackers and hacktivists to state-sponsored threats. According to Verizon's *2019 Data Breach Investigations Report*, the biggest threat to the public sector is state-sponsored cyberattacks. More than half of the incidents in the Verizon study were reported by public sector employees, with 330 incidents resulting in confirmed data disclosure. State-sponsored attacks, miscellaneous errors and privilege misuse represent 72% of public sector breaches, with espionage and financial gain reported as the two primary motives.

Top government business concerns include availability/staying open for business, protecting sensitive data and lack of expertise and resources to manage complex protection, according to Radware's *2018–2019 Global Application and Network Security Report*.

Staying Open for Business

Government institutions depend on websites and online services. Their networks and applications must be available 24x7 to allow consumers to access resources, especially during critical time periods. Government respondents to the aforementioned Radware report stated that malware and bots, distributed denial of service (DDoS) and social engineering are the most frequent types of attacks. More than half reported productivity/operational loss, followed by loss of brand reputation and negative customer experience as repercussions of successful attacks.

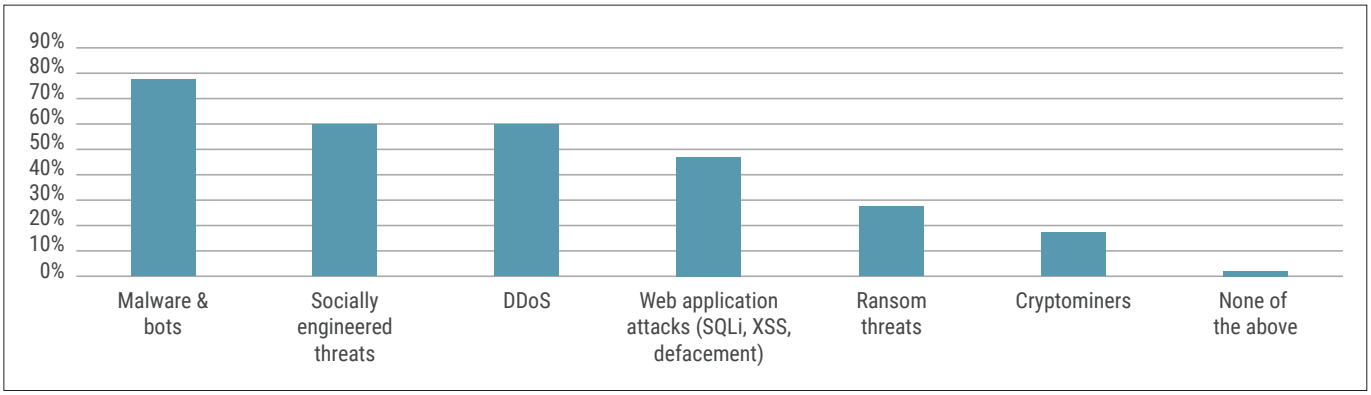

Figure 1: Types of attacks experienced (2018)[1]

[1]*2018–2019 Global Application and Network Security Report*

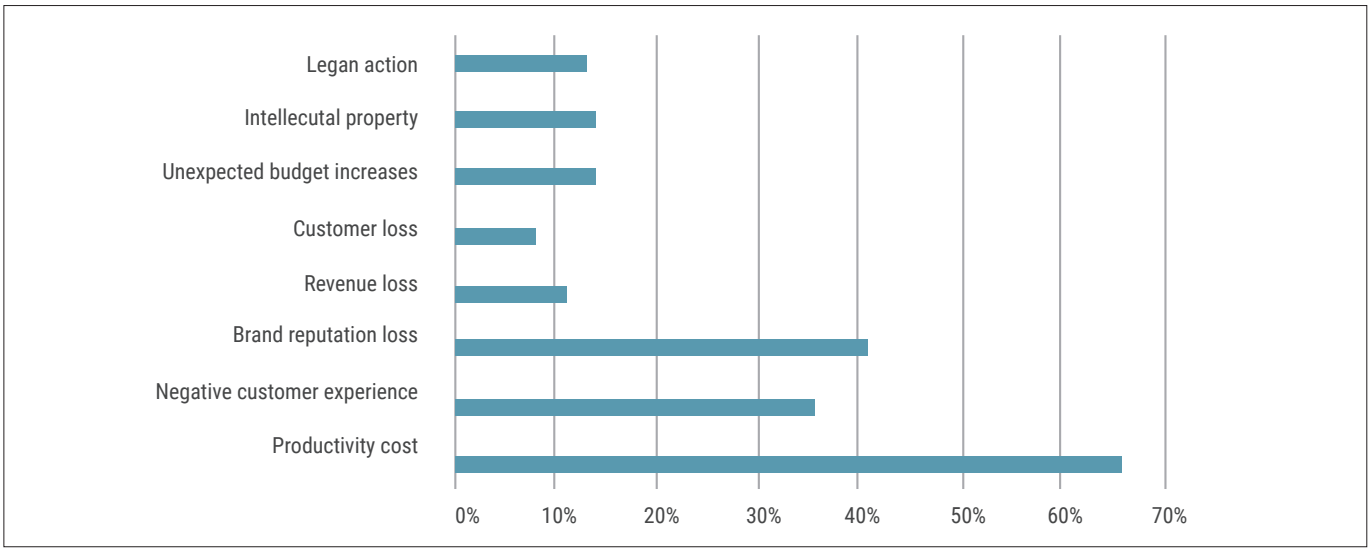

Figure 2: Repercussions of successful attacks (2018)[2]

Because government institutions are dependent on their applications, it comes as no surprise that application vulnerabilities were identified as the top threat (34%) that IT managers are concerned about. Security and ease of use of applications must be on par with the standards set by applications such as Google, Amazon and Netflix.

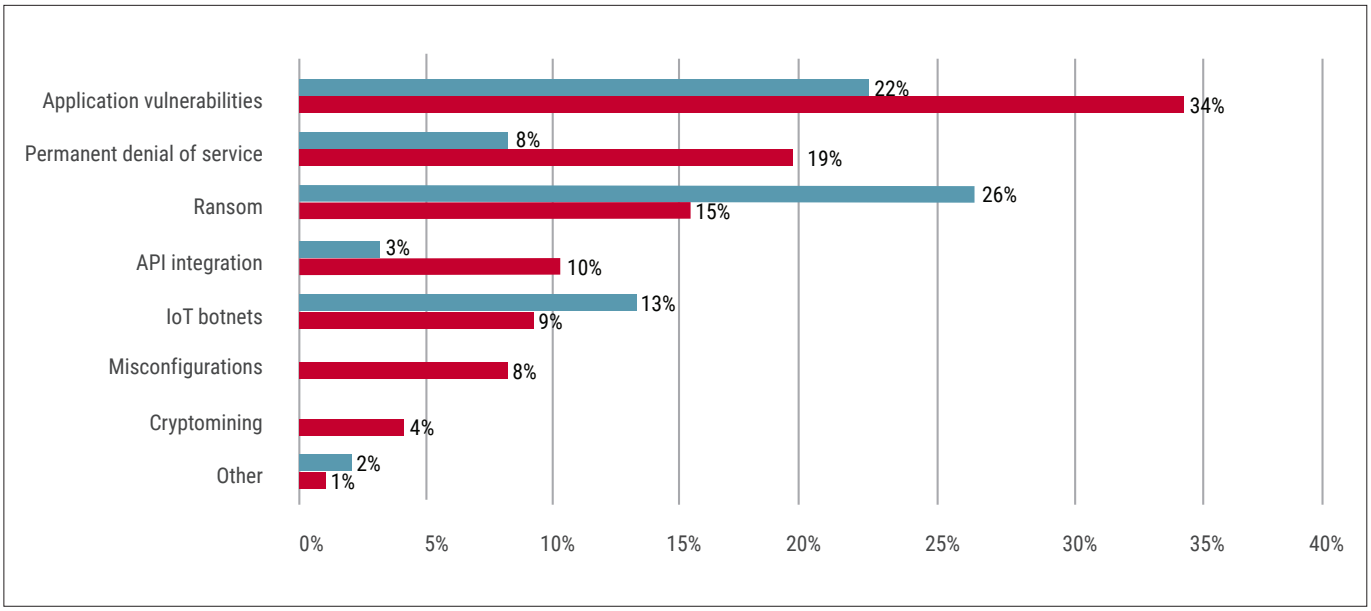

Figure 3: Perception of the biggest threats in the coming years[3]

[2]2018–2019 Global Application and Network Security Report
[3]2018–2019 Global Application and Network Security Report

Protecting Sensitive Data

Government institutions process and store large volumes of personal information. Verizon's 2019 *Data Breach Report* indicates that "Cyber-espionage is rampant in the public sector, with state-affiliated actors accounting for 79% of all breaches involving external actors. Privilege misuse and error by insiders (employees) account for 30% of breaches."

Based on Radware's survey, data leakage is the top business concern of government professionals when faced with a cyberattack, followed by service outages, reputation damage and revenue loss.

Government institutions continue to move applications and data to the public cloud. While this move transforms infrastructure operations, improves the user experience and reduces costs, there is less control and visibility to manage and secure applications hosted in cloud environments. Based on the aforementioned Radware report, one-third of government respondents reported web and application intrusions as the top cloud computing concern, followed by insider threats and misconfigurations.

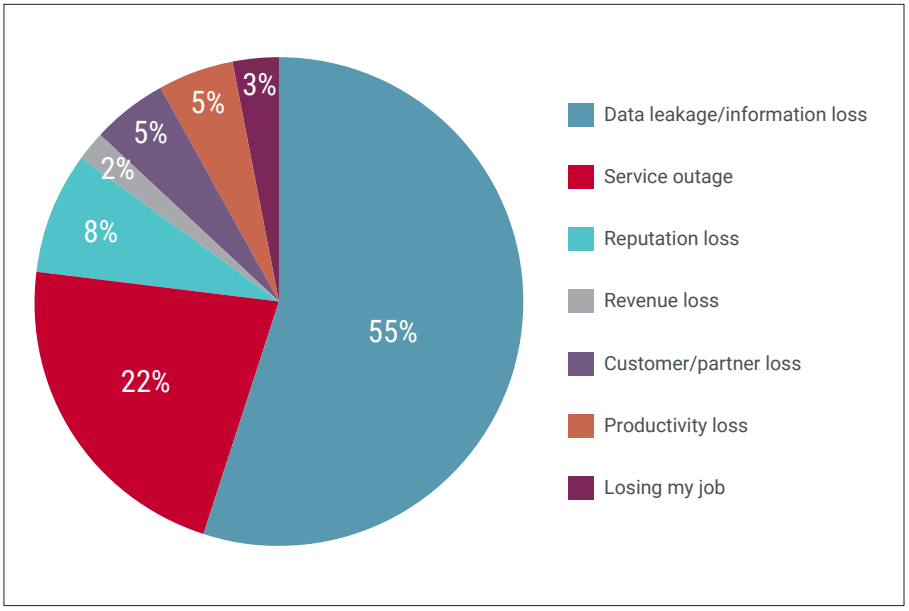

Figure 4: Biggest government concerns if attacked[4]

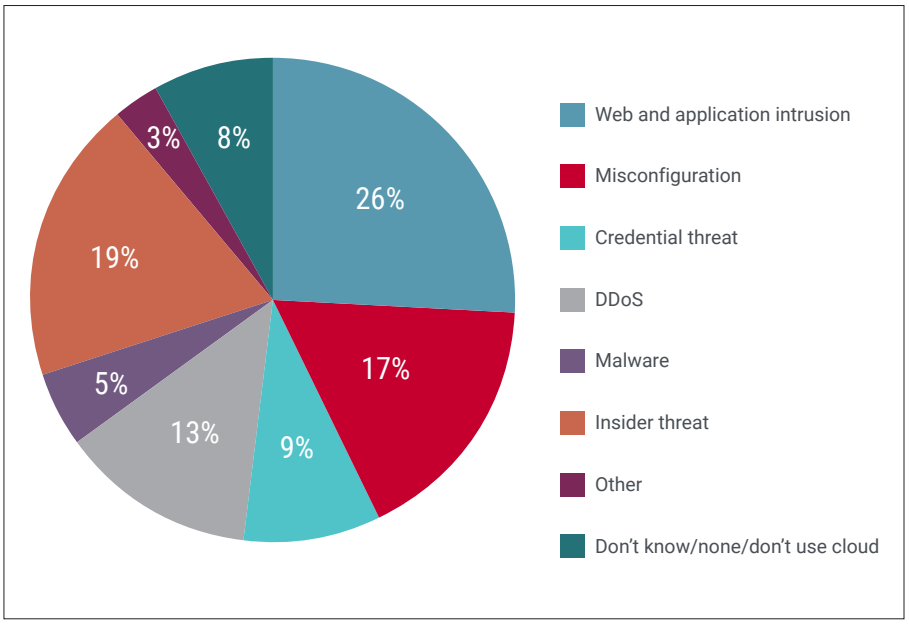

Figure 5: Top security threats to government cloud environment[5]

[4]2018–2019 Global Application and Network Security Report
[5]2018–2019 Global Application and Network Security Report

Government data centers must adhere to numerous guidelines, including the Federal Risk and Authorization Management Program, International Traffic in Arms Regulations (ITAR) and Criminal Justice Information Services (CJIS). Institutions have to comply with evolving regulations and standards, such as Payment Card Industry (PCI) and General Data Protection Regulation (GDPR). Encryption protocols are required to secure transactions, but attacks using encryption are also a concern, growing 13% in 2018, according to the *2018–2019 Global Application and Network Security Report*.

Lack of Expertise and Resources to Handle Complex Threats

Although keeping websites, data and the network secure is critical, it is becoming increasingly difficult because of the cybersecurity skills shortage and the increasing array of attack vectors. Based on the *2018–2019 Global Application and Network Security Report*, 63% of security teams are exhausted after a 24-hour attack.

Government customers have three main concerns regarding managing security resources:

- Having the staff and tools to keep up with the volume of attacks and threats.
- Government agencies are adversely affected by the cybersecurity skills shortage because they have more difficulty attracting talent than the private sector.
- IT budgets are particularly tight in the government sector due to budget cuts and the need to show return on investment.

CASE STUDY:

A national law enforcement agency needed to construct a new data center that potentially required a very complex network infrastructure design based on the agency's security needs. This complexity would have made it difficult for the agency's IT team to manage and update the various subsegments with its current resources.

To meet the customer's requirement of separate subsegments and avoid the cost of building a segmented network infrastructure, Radware proposed segregation of each department's applications by virtualizing its application delivery controller (ADC) and web application firewall (WAF) functions. Each department would have its own virtual ADC reserved for its own dedicated resources. Each ADC would get its own WAF, so each department would receive its own security policies for the set of applications that it protects.

This virtualized solution increased flexibility and lowered the total cost of ownership (TCO) of the new data center by avoiding the implementation of a complex physical network infrastructure.

SOLUTION SUMMARY — WHAT YOU SHOULD CONSIDER

Government institutions face many operational and security challenges. Radware has more than 20 years of experience leveraging cybersecurity research to provide solutions that solve business and technology challenges. Radware solutions have the industry's most expansive set of compliance certifications, including PCI, HIPAA, GDPR and advanced ISO regulations, to address data security in the cloud, including application and malware protection and encrypted traffic inspection.

For concerns with availability, Radware offers a behavioral-based hybrid attack mitigation service, which combines on-premise detection and mitigation with cloud-based volumetric attack scrubbing as well as a fully managed cloud-only attack protection service. In addition, keyless SSL attack protection defends against encrypted attacks without adding latency and impacting legitimate traffic. Radware's ADC ensures availability and disaster recovery for local and globally-dispersed applications while providing scalable architecture and automation across multiple heterogenous environments.

To protect sensitive data as well as mission-critical web applications and APIs, Radware's WAF solution, available on-premise or managed in the cloud, uses a positive security model and machine learning algorithms to provide an adaptive defense

against the OWASP Top 10 and other threats. Radware's WAF integrates with the hybrid attack mitigation solution and Radware's Bot Manager, which provides precise bot mitigation and management.

For security and control over assets in multiple public cloud environments, Radware's Cloud Workload Protection Service provides one solution to identify exposed assets and remove excessive permissions, detect misconfiguration issues and detect and defend against data breaches.

To assist with resources and expertise, Radware's automated attack mitigation and WAF solutions use machine learning, real-time signature creation and auto-policy generation to shorten time to mitigation by automatically mitigating attacks.

Radware's Emergency Response Team (ERT) offers a fully managed network and application security service 24x7, which includes immediate response, onboarding, consulting, remote management and reporting. The ERT offers threat intelligence subscriptions designed to provide actionable real-time data for immediate protection against active suspicious attacks and attackers.

About Radware

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis of DDoS attack tools, trends and threats.