SECURITY FROM THE INSIDE OUT

How cloud-based access control offers a new model for simplifying and strengthening network security

Ransomware may top today's list of security concerns for government IT, but it shouldn't divert attention from the ongoing threat of website and application disruption or data theft. Hackers and identity thieves know that government applications and data may be an easy target:

- Public sector entities are the third most prevalent victims of data breaches[1]
- Cyber criminals stole nearly 1.2 million personal identities from public administration organizations in 2016[2]
- Public entities have paid millions of dollars in breach-related lawsuit awards and fines[3]

Securing the network is still a critical challenge for government IT teams. Although cybersecurity has many dimensions, it starts with how users log into and navigate the network to access sensitive information and application services.

MORE USERS, MORE POINTS OF VULNERABILITY

Every year, more employees and contractors work away from traditional offices and worksites. This trend requires secure remote access to applications and data, which presents challenges for IT departments and users.

Determining who can access what and where. Remote access creates vulnerabilities because once logged into a network, users often have a free-range path to multiple applications, databases and network-connected systems. Hackers take advantage of this openness by using legitimate single sign-on credentials to masquerade as an authorized user for a less-sensitive application. Once in the network, they can move laterally to steal data or install malware in a critical application.

Use Cases for Cloud-Based Access Control

A remote access solution in the cloud offers distinct capabilities in four IT use cases.

USER ACCESS CONTROL.
Supports the convenience of single sign-on and multifactor authentication while controlling application access. Automatically terminates access to published applications when an employee leaves or a contractor's work is complete.

SECURE ACCESS TO LEGACY APPLICATIONS.
Provides access to legacy client/server applications that lack the latest security or performance capabilities to support public web access.

RISK AWARENESS.
Offers scalability for monitoring application and data access by thousands of users to detect risky behavior and unintentional data exposure.

WEB APPLICATION ACCESS.
Provides a flexible and extensible way to deploy access to web (e.g., HTTP and SSH) as well as virtual network computing (VNC) and remote desktop protocol (RDP)-based applications without requiring complex hardware or software installations.

For example, the widely reported theft of point-of-sale system data from a popular retailer may have been initiated by a hacker leveraging an AC/heating contractor's user credentials to manage the company's air handling system.[4]

Simplifying the user experience. One way to strengthen security is to make users do more to prove their identity before granting network access. Yet security measures such as multifactor authentication often confuse and frustrate users, increase the network cost per user, and add to the management and support burden for IT.

Avoiding management complexity. Most controls for remote access focus on the network perimeter with a virtual private network (VPN) solution. However, this approach requires IT to spend time and resources to manage the complex and costly hardware and software infrastructure, policies and access lists involved. In a large organization, it can be hard for IT to keep up with VPN user accounts that should be closed, which creates another point of vulnerability.

These challenges — and the security gaps they create — will only increase as organizations outsource more non-core functions, support more user mobility and offer more services.

TRADITIONAL ACCESS TECHNOLOGIES ARE A BIG BURDEN

Remote access may be a simple concept, but implementing it has not been an easy task. Granting network access to a user for even one application has usually required IT to set up a corporate owned laptop; configure privileges in the enterprise user directory system; and deploy client certificates, VPN software and mobile device management to secure that deployment. These and the other complex steps all come with their own deployment and configuration challenges which leave administrators seeking a secure but simplified method to achieving remote access functionality.

Access controls, firewall rules, VPN management systems and multifactor authentication methods and other on-premises security systems create other challenges. These technologies are difficult for IT to maintain and they typically don't provide centralized visibility into user access and activity across internal and web applications after their initial VPN connection is made.

THE NEW APPROACH: ACCESS CONTROL IN THE CLOUD

The cloud allows government agencies to move beyond the limitations of traditional, premises-based technologies for remote access. Government IT teams can now consider a cloud-based, software-as-a-service solution that simplifies application access and security controls without providing access to the entire network. The solution begins when the user signs in to the cloud service, which then delivers authorized applications to the user's browser over HTML5, regardless of where the applications are hosted. Users can be authenticated with the agency's internal user directory system or an external identity provider (IdP) service.

By virtualizing the user connection to applications instead of providing direct network access, the cloud access solution can stop malware before it enters the network. The cloud simplifies access management by eliminating VPN connectivity issues, device incompatibilities, custom scripts and the need to integrate multiple security tools. The solution can also take advantage of cloud features for high-availability, server load balancing, automatic application routing, access scalability, web application inspection, and application deployment across public and private cloud environments.

With access control in the cloud:

- Lateral movement within the network is no longer possible
- Users can access authorized applications from any device and browser without VPN client software or browser plug-ins
- Agencies have predictable costs and easy scalability through a subscription-based model
- There is no need for on-premises hardware or software

Akamai's Enterprise Application Access Service

The remote access method provided by the Akamai Enterprise Application Access service allows remote users to connect to internally hosted, sensitive web applications and services without the need to open inbound ports on your firewall for traditional VPN connectivity. This design means you can reduce the attack surface of an externally facing network as well as securely deploy applications to any authorized user. And because of the simplified method developed by Akamai, the deployment process takes only a few hours.

Endnotes

1. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
2. https://www.symantec.com/security-center/threat-report
3. http://www.govtech.com/opinion/Whats-at-Stake-When-Governments-Data-Is-Stolen.html
4. http://money.cnn.com/2014/02/06/technology/security/target-breach-hvac/index.html

This piece was developed and written by the Center for Digital Government custom media division, with information and input from Akamai.

Produced by: Center for Digital Government

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century. **www.centerdigitalgov.com.**

For: Akamai

Akamai is the leading cloud platform for helping government agencies and higher education organizations provide secure, high-performing user experiences on any device, anywhere. Akamai removes the complexities of connecting the increasingly mobile world, supporting 24/7 consumer demand, and enabling government agencies and higher education institutions to securely leverage the cloud.