Security in Cloud Computing

Sabrina Slattery and Ron Griffiths

Recap and Overview

Last week: Automation

Where and how it's used

Threats to automated systems

How to secure these systems

This Week: Cloud Computing Security

New Advancements in Cloud Computing

Current and Future Models of Threat Detection

Securing the Cloud

Intro to Endpoint Protection

Cloud- based endpoints are any final destination cloud data reaches (i.e. smartphones, laptops, etc).

Cloud security strategies must be all-encompassing , covering any and all possible points of attack.

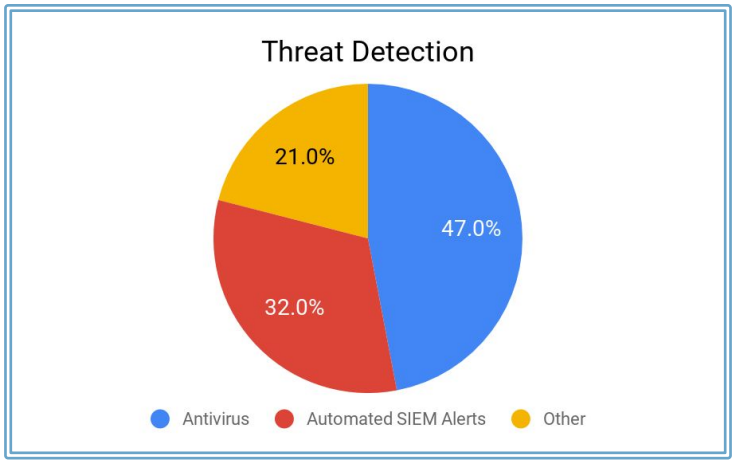
Sensitive data comprises 21% of all data stored on the cloud–an increase of 17% from the past few years

60% of cloud-based endpoints now connect to the network - this includes IoT and mobile devices, desktops, servers, wearables, and cloud-based apps. The drive to have computing available anywhere and at any given time is causing cloud-based tech to progress at a faster rate, opening new windows of vulnerability.

31.3% of an organization's security attacks per month are directed towards the cloud–an average increase of 27.7% from last year

Endpoint Protection - DDoS Attacks within the Cloud

UIs and APIs are some of the biggest challenges when securing the cloud.



Misconfigurations is a major contributor to leaks, breaches, and loss of data for users with information stored in the cloud.

Endpoint Protection - Control and Data Management

The McAfee Data Loss Prevention (DLP) is a tool which can help organizations monitor data, protect against vulnerabilities, and alleviate the impact of malicious attacks.

Some Statistics:

- 42% of respondents report their endpoints have been breached
- 17% of breaches involved 10-24 endpoints
- 63% of respondents report remediation of a single endpoint takes an avg of 24 hours or less

Endpoint Protection - Visibility, Compliance, and Data Protection

Security teams need visibility within the cloud, so as to identify user activity from malicious activity.

Teams will need to adopt a cloud access security broker (CASB) solution, helping with visibility and compliance issues.

Enforces encryption, tokenization, and access control–detecting and responding to all types of cyber threats within the cloud.

Some of the most common threats exploiting cloud-based endpoints:

63% Web 'Drive-Bys'

53% Social Engineering

50% Ransomware Wring/Phishing

Endpoint Protection Takeaway

Takeaway: When implemented correctly, CASB solutions will be able to protect data from all sides of the cloud.

This endpoint security solution is integral for safeguarding the cloud –

Organizations must augment their abilities to more proactively defend their systems and detect threats earlier in the cyber kill chain.

New Technologies in Cloud Computing Security Systems

Pre-Existing Solutions:

- Machine Learning and AI Security measures
- Multi-Agent Systems
- Security Algorithms
- DES (Data Encryption Standard)

Solutions Being Researched:

- AES and Blowfish Algorithm combination
- Facial Recognition Authentication for Cloud Computing
- PKI Mechanisms protecting NFV technology

New Technology - AES and Blowfish Algorithms

Algorithm	Key Size	Block Size
DES	64 bits	64 bits
AES	256 bits	128 bits
Blowfish	32-448 bits	64 bits

Key: AES - Advanced Encryption Algorithm; DES - Data Encryption Standard

Source: Utkarsh Gupta et al. (2018). Enhancement of Cloud Security and removal of anti-patterns using multilevel encryption algorithms. *International Journal of Recent Research Aspects*. 7(1), 55-61.

New Technology - Facial Recognition Authentication

Also known as Biometric Authentication

Currently being used to unlock devices and authorizing personnel within high-security areas

Proposed for access to a user's data and information within the cloud for an added layer of security

New Technology - PKI Mechanisms

Abbreviated Terms:

PKI (Public Key Interface)

NFV (Network Function Virtualization)

VNF (Virtual Network Functions)

Concerns with NFV in Cloud Computing:

1) No mutual authentication between VNFs and element management
2) VNF services data leakages through fake or contaminated VNFs
3) Data consumption attack due to a contaminated VNF

How PKIs can help:

- PKIs provide extreme security and are **triple authorized** (certificate of authority (CA), registration of authority (RA), and validation of authority (VA))
- Guaranteed secure data from the user directly to the cloud

References

Endpoint Security | McAfee Products

Gupta, Utkarsh, Shivani Saluja, and Twinkle Tiwari. 2018. “Enhancement of Cloud Security and Removal of Anti-Patterns Using Multilevel Encryption Algorithms.” *International Journal of Recent Research Aspects* 5 (1): 55–61. http://search.ebscohost.com.westvalley.idm.oclc.org/login.aspx?direct=true&db=a9h&AN=129311331&site=ehost-live.

Hawedi, Mohamed, Chamseddine Talhi, and Hanifa Boucheneb. 2018. “Multi-Tenant Intrusion Detection System for Public Cloud (MTIDS).” *Journal of Supercomputing* 74 (10): 5199–5230. doi:10.1007/s11227-018-2572-6.

Park, Sangho, Hyunjin Kim, and Jaecheol Ryou. 2018. “Utilizing a Lightweight PKI Mechanism to Guarantee a Secure Service in a Cloud Environment.” *Journal of Supercomputing* 74 (12): 6988–7002. doi:10.1007/s11227-018-2506-3.

Sorapak Pukdesree, and Paniti Netinant. 2018. “Reviewed: The Face Authentication Processes for Accessing Cloud Computing Services Using IPhone.” *TEM Journal* 7 (3): 475–79. doi:10.18421/TEM73-01.

Questions?