ACI UNIVERSAL PAYMENTS

THE AVC'S OF CLOUD SECURITY

Lisa McKee, CISA, ISA, PCIP
NEbraskaCERT CSF

May 15, 2019

What is your Business's Cloud Appetite?

1. Already in the cloud?
2. Considering moving to cloud?
3. No intentions of cloud computing?

The AVC's of Cloud Security

- **Architecture**
  - Ownership of hardware
  - Dedicated/Multi-tenant
  - Data diagrams
  - Data center locations
- **Access Controls**
  - Management
  - Role based
  - Term/Inactive users
  - User authentication
- **Asset Inventory**
  - List of devices
- **Audit**
  - Logs
  - Right to audit
    - On-site audits
    - Frequency
    - Findings
- **Vulnerability Management**
  - Scanning
  - Patching
  - Penetration testing
  - Rogue access points
  - Rules of engagement
  - Exception management
- **Vendor Management**
  - Due diligence reviews
  - Risk ratings
  - Compliance
  - Vendor evaluation
- **Contracts**
  - Roles & Responsibilities Matrix
  - SLA's
  - Recovery time requirements
  - Data storage locations
  - Right to audit clause
  - Breach notification requirements
  - Incident definition and resolution
  - Compliance requirements
- **Controls**
  - Policies/Procedures
  - Encryption/Transmission
  - Anti-virus
  - Internal Devices
- **Compliance**
  - Data privacy requirements
  - International, state, local
  - Customer requirements

Why This is Important?

UpGuard Products Insights Customers Login Free demo

Cloud Leak: How A Verizon Partner Exposed Millions of Customer Accounts

Last updated by Dan O'Sullivan on December 12, 2018

Tweet Share Like 644 Share

While this blog post provides a description of a data exposure discovery involving NICE Systems and Verizon, this is no longer an active data breach. The UpGuard Cyber Risk Team notified Verizon of this publicly exposed information and action was ultimately taken, securing the database and preventing further access.

UpGuard's Cyber Risk Team can now report that a misconfigured cloud-based file repository exposed the names, addresses, account details, and account personal identification numbers (PINs) of as many as 14 million US customers of telecommunications carrier Verizon, per analysis of the average number of accounts exposed per day in the sample that was downloaded. The cloud server was owned and operated by telephonic software and data firm NICE Systems, a third-party vendor for Verizon.

Cloud database removed after exposing details on 80 million US households

Exclusive: The cache included information on addresses, income levels and marital status.

BY LAURA HAUTALA
APRIL 29, 2019 12:12 PM PDT

LEER EN ESPAÑOL

- https://www.google.com/amp/s/www.upguard.com/breaches/verizon-cloud-leak%3fhs_amp=true
- https://www.cnet.com/news/cloud-database-removed-after-exposing-details-on-80-million-us-households/

Compliance

- Understand your compliance landscape
  - Data privacy requirements
  - International regulations
  - State/Local Laws
  - Legal, HR
  - Industry standards
- Customer compliance requirements
  - PCI, GDPR, ISO, Data Privacy

Vendor Management

- Due Diligence Reviews
  - Financials
  - Data Breach
  - Compliance
  - Physical Security
  - Information Security
  - DR/BCP
  - Reputation/Brand
  - Mergers/Acquisitions
  - DHS Threats
- Risk Ratings
  - H/M/L
  - Essential/Critical/Non-Essential
- Compliance
  - PCI, GLBA, ISO, SSAE, Industry Standards
  - Managing non-compliance
- Vendor Evaluation
  - Processes/procedures for overall approval/denial of a vendor
  - Escalation processes

Contracts

- **Roles & Responsibility Matrix**
  - Clearly define and articulate who is responsible for what tasks
  - Access controls, vulnerability management, audit logging, etc.
  - Sign-off and approval by both parties
- Service Level Agreements (SLA's)
  - Define SLA expectations
  - Penalties for not meeting SLA's
  - Reporting issues
- Recovery Time Requirements
  - Disaster recovery and business continuity requirements
  - Lost revenue if system is down and unable to function
  - Fines/penalties for system outage(s)
- Data Storage Locations
  - Where is data stored?
  - Data across borders
  - How is data stored/transmitted, encrypted?

Sample Roles & Responsibility Matrix

Steps to Determine Responsibility	Discussion Points	Entity	TPSP	Evidence to be Provided
System Components (e.g., Firewalls, Servers, Applications, Appliances)				

Determine the procedures for the design, staging, implementation, and ongoing maintenance of system components.	• Firewall Reviews
	• Encryption of transmissions over public networks and end user messaging systems
	• System updates and maintenance including
	  ○ Patching cycles
	  ○ Operating system vs. application
	  ○ Virtual vs. physical
	  ○ Centralized tools and reporting
	• Isolation strategies (segmentation, intrusion detection/prevention)
	• Change management procedures
	• Anti-virus deployment strategies
	• Change-detection strategy for critical files
	• Risk-based analysis including risk-assessment results
	• Access control procedures
	• Defining roles
	  ○ Approval process
	  ○ Entitlement reviews
	  ○ Revocation procedures
	  ○ Two-factor requirement
	  ○ ID and password requirements
	  ○ Session timeouts and login requirements
	  ○ Incident response
	• Time synchronization (Network Time Protocol)			

Contracts

- Right to Audit Clause
  - Right to perform on-sight assessment annually or if an event triggers the need sooner
  - Not responsive to annual request for vendor management due diligence reviews
  - Something in the annual review does not seem right triggering the need for a review
  - Vendor risk ranking warrants the need for onsite assessment
  - Data breach occurred
- Breach Notification
  - Who do you contact and who do they contact in the event of a breach
  - Reporting time
- Incident Definition and Resolution
  - Define what constitutes an incident, ensure this meets compliance requirements
- Compliance Requirements
  - Data across borders
  - Data centers
  - Compliance adherence PCI, GDPR, ISO, FFIEC
- Vendors
  - 3rd/4th/5th party vendors data is shared

Architecture

- Dedicated or Multi-Tenant (Shared Hosting Provider)
  - Know what kind of environment you are getting
  - Dedicated = everything in the environment is specific to your organization
  - Multi-Tenant = customers have individual logon credentials but their data is intermixed in storage, hardware is shared
- Ownership of Hardware
  - Dedicated environments who is providing the servers and network devices?
  - HSMs or any other equipment treated differently?
- Data Center Locations
  - Know where they are located, some regulations have requirements for DC in country
  - Ensure it meets the business requirements
- Data Diagrams
  - ****Current diagrams for all assets in the environment that shows ownership**

Controls

- Policies/Procedures
  - Data retention
  - Training
- Encryption/Transmission
  - Requirements
- Anti-virus
  - Tools
  - Management
- Internal Devices
  - Servers, HSM's, Printers, Domain Controllers, Storage Devices, etc.
  - Build configuration
  - Management
  - Logging

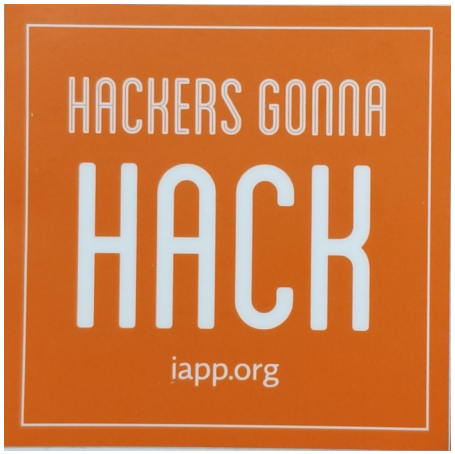
Asset Inventory

- ****Current list of all systems, applications and devices in the environment**
  - Must include vendor managed assets
  - Policies/procedures for retirement of assets when appropriate

NOTE: Assets in the data diagrams, asset inventory, vulnerability scans and penetration testing should all match.

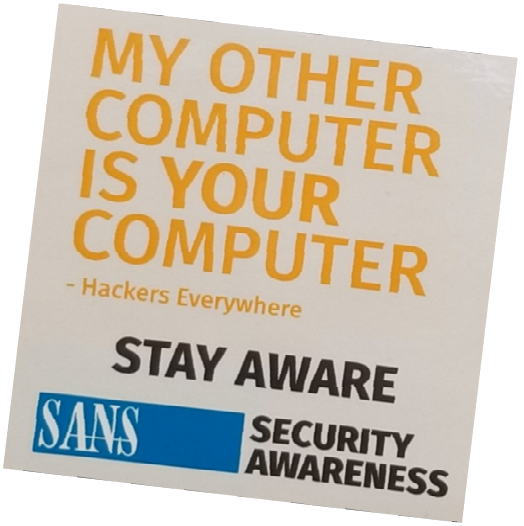
Access Controls

- Management
  - Who is responsible for oversight of the access control system?
  - Physical access to the data center, rack, cage, etc?
- Role Based
  - Least privileged
  - Reviewed every 90 days
  - Policies for managing contractors and employees
- Term Users
  - How are termed and inactive users managed?
  - Should have the same rules, policies for managing access controls
- Users Authentication
  - Multi-factor authentication to access all sensitive/private information



Vulnerability Management

- Scanning
  - Are there restrictions on vulnerability scanning?
- Patching
  - Patching schedule
  - Who is responsible for applying patches?
- Penetration Testing
  - Limitations on internal penetration testing?
- Managing Access Points
  - Who scans the environment for unauthorized access points?
- Exception Management
  - How will exceptions be managed?
- Rules of Engagement
  - Document that defines what is allowed, when, by whom, etc. for each category
  - Processes for reporting a vulnerability



Audit

- Logging
  - All critical systems are logging all critical events
  - Logs written to centralized server
  - ****In the event of a breach, can you retrace what happened?**
- Right to Audit
  - On-Site Audits conducted per the contract or if an event triggered the need
  - Frequency
    - Yearly, Bi-Annual, etc.
  - Findings
    - Documented policies and procedures for managing findings from on-site audits
    - Remediation and retesting
  - Exceptions
    - Exception management processes which allow for escalation if necessary

Cloud Security Strategy Tips

- Know your compliance requirements
- Know your customers
  - Where they are located
  - Contract provisions
  - Compliance requirements passed through to you
- Detailed, clear, concise contracts with Cloud vendor
- Engage with legal and/or outside counsel
- Thorough Vendor Management Program
- Cloud implementation plan

Don’t be the next data breach!

Questions

Lisa McKee
ACI Worldwide
Lisa.McKee@ACIWorldwide.com
https://www.linkedin.com/in/lisammckee/