Cybersecurity in Payroll

Anatomy of a Breach and How to Prepare

2023 Asure Reseller Partner Conference

Asure

Speaker Introduction

Joshua Gohman, CISSP

VP, Information Security

- Over 20yrs IT, Cybersecurity, and Risk Management experience beginning in the US Army and continued in civilian career leading security consulting teams conducting technical security assessments, security and compliance audits, and security program implementations for companies of all sizes from startups to Fortune 500 companies.
- Joined Asure in 2018 led the security team in developing a world class information security program establishing security best practices, implementing security tooling to protect systems, and leading our Incident response to security and disaster recovery events.

Cybersecurity in Payroll

01 Anatomy of a Breach

02 What to Do Now?

03 Lessons Learned

04 Securing Payroll

Anatomy of a Breach

Attack Scenarios

01

User Email Compromise

1. Phishing Attack – Credential Harvesting
2. Compromise user email accounts
3. Resets user's password in the payroll system via self service password reset
4. Attacker Logs in and Updates bank info
5. Waits until regular payday

02

Phishing Attack

1. Phishing Attack – Credential Harvesting
2. Compromise client email accounts
3. Change rules to deliver mail from SBO to separate folder
4. Urgent request to setup new EE/1099
5. Out of Cycle Payment or Payroll

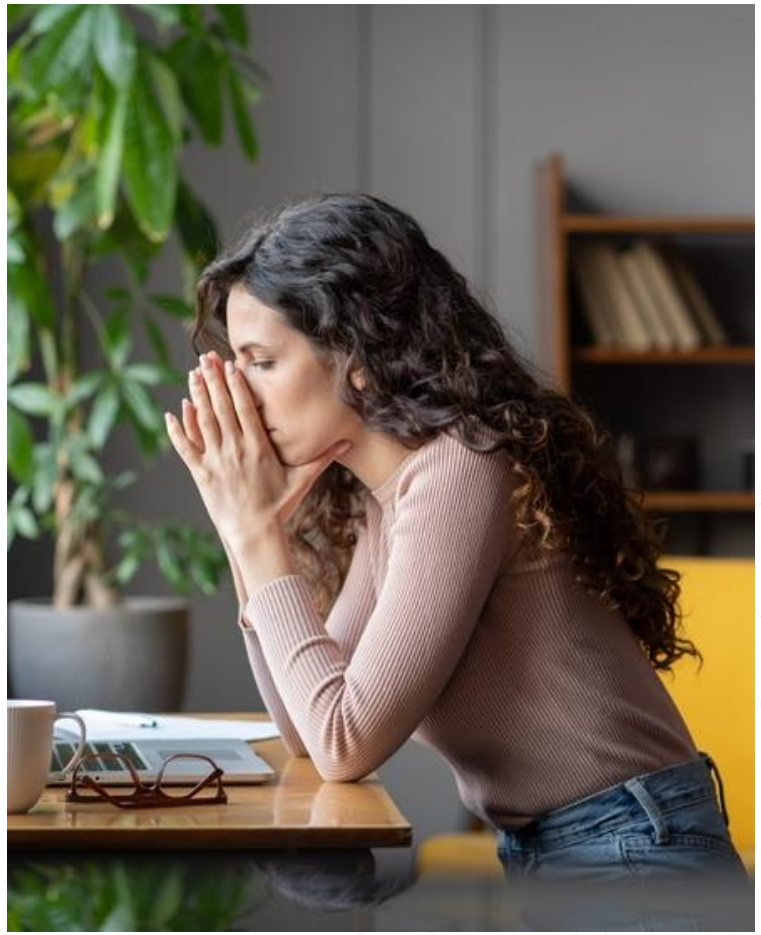
03

New Client Setup

1. New client setup
2. Fake EE and company docs
3. Goes through implementation
4. Once moved to DD, NSFs company payment

I've Been Breached – What to do now?

- Call the bank and try to get a reversal
- Secure Evidence
  - Screenshots from Classic with exact dates and times of audit events
- Contact Support with all the information
  - Support will work with Security team to provide IP addresses of the events in question
- Contact the FBI or the Secret Service



Lessons Learned

- Security best practices aren't just for the payroll system or the Service Bureau – train your clients
- Security in layers – Defense in Depth
  - People, Processes, Technology
- Onboarding/Implementation
  - Credit Checks
  - Set limits for max payroll, max dollars/check, max hours/check – set limits to "Stop" not "Warn"
- Separation of Duties
  - Distinct roles for CSR and Cash Management
  - Approval process for over limit payrolls or out of cycle payrolls
- Role based Access Controls

5 Actions to Prevent a Breach

1 Onboarding & Implementation

- Credit Checks – use to establish Payroll timelines
- Set Limits – Max Dollars/Max Hours – Set to Stop not Warn

2 Separation of Duties

- Distinct Roles for each job function
- Approval Process for out of cycle or large payrolls

3 Role-Based Access Controls

- Separate and distinct roles for each Job function
- Do not Assign permissions directly to a user – Use a group

4 Audit Users Quarterly

- Audit SBO and remote users Quarterly to ensure that only valid users have access to the system

5 Defined Process for Granting Access

- Have a process for adding users to the system and for approving changes

What is Asure Doing?

- Building and Deploying a new Identity Management Solution
- Implementing AI/ML Fraud Detection service to detect Account Takeovers
- Enhancing MFA with AsureID – No more email
- Centralized auditing and monitoring of user logins
- Session Management – Log out users remotely

EVOLVE
An HCM Growth Summit

Q & A

Resources & Contact

Joshua.Gohman@asuresoftware.com

Fernando.Munoz@asuresoftware.com

https://www.ic3.gov/

https://www.secretservice.gov/investigation

EVOLVE
An HCM Growth Summit

Thank You!

2023 Asure Reseller Partner Conference

Asure