A Developer's tour of Cybersecurity Incident Response

Presentation by Edward Delaporte
Office of the CIO, University of Illinois

Why Listen to Me?

- 25 years in Professional Software Development
- 18 with a Cybersecurity focus

Why Listen to Me?

- 18 Years of Incident Reponse Experience

What is My Motive?

- I like to get invited to a lovely pleasant incident response.

During a Security Incident

What do developers appreciate during a security incident?

- Ready-made parking pages for each app
  - `cp 503_Unavailable.html $WEB_ROOT/index.html`

During a Security Incident

What do developers appreciate during a security incident?

- Ready-made parking pages for each app
  - `cp 503_Unavailable.html $WEB_ROOT/index.html`
- High quality logs
  - Cybersecurity, Logging Practices for Application Developers

During a Security Incident

What do developers appreciate during a security incident?

- Ready-made parking pages for each app
  - `cp 503_Unavailable.html $WEB_ROOT/index.html`
- High quality logs
  - Cybersecurity, Logging Practices for Application Developers
- Support from Cybersecurity allies
  - `securitysupport@illinois.edu`

After a Security Incident

What do developers appreciate after a security incident?

- Agile ability to deploy
- Easily rotated keys
- Keys with limited impact

Let's Have a Security Non-Incident

How can developers prepare before an incident?

- Add `.well-known/security.txt` to each server.
  - Example security.txt

Let's Have a Security Non-Incident

How can developers prepare before an incident?

- Add `.well-known/security.txt` to each server.
  - Example security.txt
- Add INFO level Security logs to each app

Let's Have a Security Non-Incident

How can developers prepare before an incident?

- Add `.well-known/security.txt` to each server.
  - Example security.txt
- Add INFO level Security logs to each app
- Adopt an SDLC

Let's Have a Security Non-Incident

How can developers prepare before an incident?

- Add `.well-known/security.txt` to each server.
  - Example security.txt
- Add INFO level Security logs to each app
- Adopt an SDLC
- Keep a ChangeLog

Let's Have a Security Non-Incident

How can developers prepare before an incident?

- Add `.well-known/security.txt` to each server.
  - Example security.txt
- Add INFO level Security logs to each app
- Adopt an SDLC
- Keep a ChangeLog
- Turn Off Stale Apps

Turn Off Stale Apps

Humor me while I preach to the choir...

How To Turn Off Stale Apps

- Keep a ChangeLog

How To Turn Off Stale Apps

- Keep a ChangeLog
- Add an End of Life Date to each `CHANGELOG.md`

How To Turn Off Stale Apps

- Keep a ChangeLog
- Add an End of Life Date to each `CHANGELOG.md`
- Document Endpoints and Data Stores in each `README.md`

What if I want to keep my app?

Keep Apps Fresh

- Adopt Code Review

Keep Apps Fresh

- Adopt Code Review
- Enable Dependabot if you use GitHub

Keep Apps Fresh

- Adopt Code Review
- Enable Dependabot if you use GitHub
- Consider the Supply Chain

Supply Chain Security Tools

- Python Index of Packages (pip) for Python: `pip audit`
- Node Package Manager (npm) for JavaScript: `npm audit`
- Composer for PHP: `composer audit`
- A recipe for a one-line audit for C#: `dotnet list package --vulnerable`

Keep Secrets

> "Alright then, keep your secrets."

Keeping Secrets

- Make More Secrets

Keeping Secrets

- Make More Secrets
- Encrypt at Rest

Keeping Secrets

- Make More Secrets
- Encrypt at Rest
- Rotate with Automation

Contact Info

`securitysupport@illinois.edu`

Edward Delaporte
Email: delaport@illinois.edu
Mastodon: https://infosec.exchange/@EdTheDev
Web: https://edward.delaporte.us/me/

Bonus Topics

Slide tool reference

https://github.com/marp-team/marp-core

Secret Management in .Net

Link Dump

> Do not use 'Secret Manager' in production.

- Azure secret best practices
- Secure authentication flows
- Overview for ASP.Net
- Securely deliver secrets as environment variables
- String replacement in `.json` files
- Another walkthrough for secrets in Microsoft IIS

Secret Management in Local Apps

- Do not hard code secrets needed by local apps.
- Prompt the user for the necessary key on the first run.
- Deliver the secret securely to the user.
- SSO is a preferred way to solve these concerns.