CROWDSOURCED REAL-TIME RISK ANALYSIS

Presented to the
NKU Cybersecurity
Symposium 2019

Justin Hall, CBTS

WELCOME

I’m Justin Hall.

I do security consulting at CBTS.

You can find me at @justinhall.

Why are we here?

Risk management isn't just done by **old white guys in boardrooms.**

We make risk decisions every day, many times **without thinking them through.**

How will this work?

I will present a **scenario**, describing the **organization** and **environment**, the **issue at hand**, and a possible **solution set***.

You will **debate amongst yourselves**. We will contribute **key questions** to consider.

Ultimately we will land on a **decision** with a **show of hands**.

SCENARIO A: MULTI-FACTOR AUTHENTICATION

The Organization

A major regional healthcare system with 4,000 employees, including administrative staff, doctors, nurses, and other caregivers. Computing environment is hybrid cloud, with some SaaS apps, some on-prem apps, mix of Windows and Linux servers, Windows clients, BYOD mobile devices.

The Problem

Employees are targeted for social engineering and credential theft. To help address this threat, the roll-out of a multi-factor authentication is proposed for use with the organization's SaaS messaging application, Exchange Online.

SCENARIO A: MULTI-FACTOR AUTHENTICATION

Solution 1:

Use **SMS-based one-time passwords** sent to employees' registered mobile phone numbers. Upon an authentication request, employees will receive a tokencode via SMS, and will type it into the application to successfully auth.

Solution 2:

Use **hardware keys** distributed to employees that can be connected to USB ports on company-owned assets, and Bluetooth keys for use with smartphones. Upon an authentication request, employees will insert/produce the key, and press a button on the key to successfully auth.

Solution 3:

Use a **smartphone app that receives push notifications**. Upon an authentication request, employees will receive a notification on their registered mobile device, and will confirm with a tap on the notification to successfully auth.

SCENARIO A: MULTI-FACTOR AUTHENTICATION

Key Questions

What are the tradeoffs around **deployment** and **ongoing management** of the solution?

How can each solution be **attacked** or **circumvented**?

Given the **user population**, how will each solution be received and integrated into daily use?

How can each solution be integrated into **other MFA use cases** besides protecting email?

SCENARIO B: TEAM CHAT

The Organization

An IT services company with 1500 employees globally. Well regarded for their technical expertise, deep knowledge of solutions and products. Fully owned subsidiary of telecom, from whom IT operations and security management are performed. Hybrid cloud and on-prem infrastructure, Windows/Mac workstations, variety of server platforms. BYOD mobile devices.

The Problem

The security consulting team operates remotely and needs to stay in communication. Given the nature of their work, sensitive customer data for which they are stewards will be among the information sent with this application. The team would use the app from company assets as well as personal mobile devices.

SCENARIO B: TEAM CHAT

Solution 1:

Use company's **officially supported SaaS** chat application**.** App's ability to address team requirements is **limited**.

Infrastructure and app support is provided by the company's IT operations group as well as the SaaS vendor.

Solution 2:

Use **unsupported SaaS** chat application**.** App's ability to address team requirements is **high.**

Infrastructure and app support is performed by the customer, as well as the SaaS vendor.

Solution 3:

Use **unsupported on-prem chat application.** App's ability to address team requirements is moderate.

Infrastructure and app support is provided solely by the customer.

SCENARIO B: TEAM CHAT

Key Questions

What are the tradeoffs around **deployment** and **ongoing management** of the solution, specifically on-prem vs. cloud, and self-managed vs. IT managed vs. vendor managed?

How can each solution be **attacked** or **circumvented**?

How **safe is sensitive data** in each solution? What control does the team retain over the data? How can likelihood of disclosure or breach be determined?

SCENARIO C: WEB BROWSERS

The Organization

A small manufacturer with one HQ facility and several small plants scattered across the US. 500 employees. Computing environment is all on-prem with servers, workstations, and network devices all operated by IT ops team. No dedicated security staff. Windows servers and workstations, company-owned mobile devices.

The Problem

Users require the use of web browsers to access company applications, for business operations, and for personal use. Users have been downloading and installing a variety of web browsing software, including Chrome and Firefox. Recently, a user’s workstation was infected with ransomware after the user visited a website that used an exploit in a Firefox ad-blocking extension to install the malware.

SCENARIO C: WEB BROWSERS

Solution 1:

Require the use of the built-in web browser for the supported OS platform, Microsoft Edge. Disallow the use of unapproved web browsers by uninstalling them when found.

Solution 2:

Install an alternative web browser on company workstations, such as Google Chrome. Allow users to use either Edge or Chrome. Disallow the use of unapproved web browsers by uninstalling them when found.

Solution 3:

Continue to allow users to install and run the web browser of their choice.

SCENARIO C: WEB BROWSERS

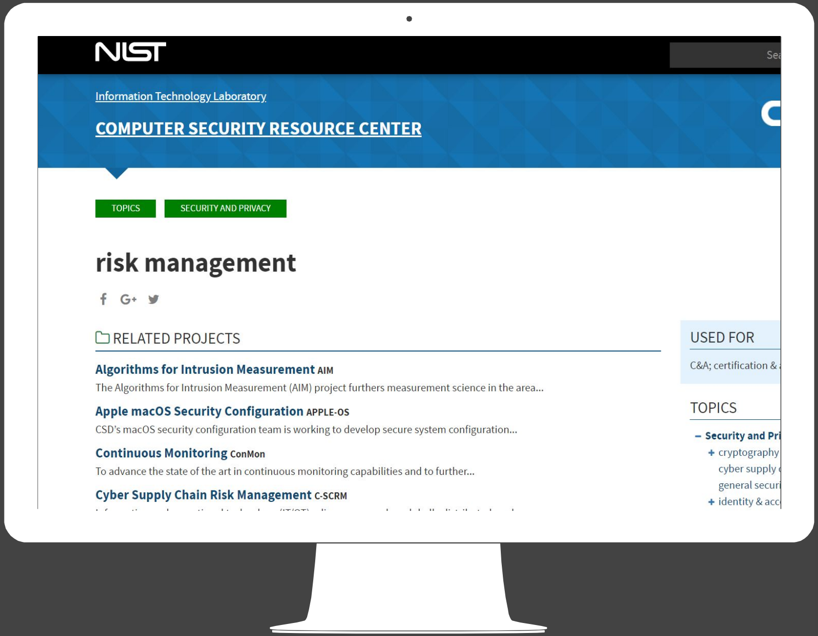
Key Questions

How would the organization deal with **keeping the solution from becoming a risk**? This includes software vulnerabilities as well as configuration flaws. Which presents the least problematic approach?

Does the use of one solution vs. another increase or decrease the **likelihood of browser-based attacks**?

How does **user preference for a specific browser** affect the decision? How might user behavior on the web change based on the solution chosen?

RISK RESOURCES



NIST

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

TOPICS | SECURITY AND PRIVACY

risk management

RELATED PROJECTS

Algorithms for Intrusion Measurement AIM
The Algorithms for Intrusion Measurement (AIM) project furthers measurement science in the area...

Apple macOS Security Configuration APPLE-OS
CSD's macOS security configuration team is working to develop secure system configuration...

Continuous Monitoring ConMon
To advance the state of the art in continuous monitoring capabilities and to further...

Cyber Supply Chain Risk Management C-SCRM

USED FOR

C&A; certification &

TOPICS

- Security and Pri
  - + cryptography
  - cyber supply
  - general securi
  - + identity & acc

NIST 800-37r2 - Risk Management Framework for Information Systems and Organizations

https://csrc.nist.gov

FAIR Risk Analysis Framework

https://www.fairinstitute.org

OCTAVE Risk Analysis Framework

https://sei.cmu.edu

THANKS!

Any questions?

You can find me at:

@justinhall

✉ justin.hall@cbts.com

linkedin.com/in/justinwhall

CREDITS

Special thanks to all the people who made and released these awesome resources for free:

- Presentation template by SlidesCarnival
- Photographs by Unsplash