Defeating Insider Attacks By Design

Subir Biswas, McAfee Canada ULC.

McAfee™

CYBERCITY CONFERENCE 10.01.19

Why this topic?

- ✓ 90% orgs feel they’re vulnerable [survey]
- ✓ 60% orgs got hit at least once in 2018 [report]
- ✓ High mitigation costs – between 100K and 500K

What is an Insider Attack?

“malicious attacks carried out by insiders who target their own organizations, mainly for confidential and sensitive business data”

Insider Threats- Categories

- ~~*Malicious*~~
- ~~*Negligent*~~
- ~~*Infiltrator*~~

- *Based on origins*
  - ✓ *S/W Development*
  - ✓ *Business Orgs.*

McAfee™

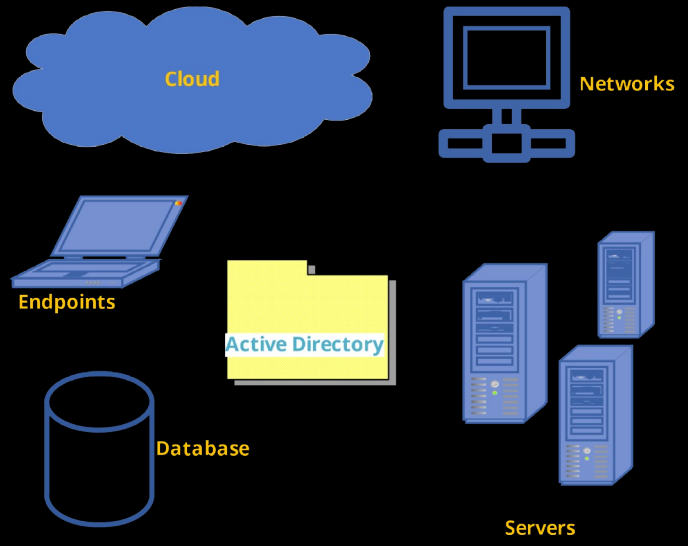
CYBERCITY
CONFERENCE 10.01.19

Insiders' Knowledge vs Targets

Insiders' Knowledge

- Privileged Account(s) Credentials
- Embedded Secret(s)
- Unresolved s/w vulnerabilities
- Design weakness/limitations
- Intellectual Property
- Access to (Signing/Debugging) Tools

Targets



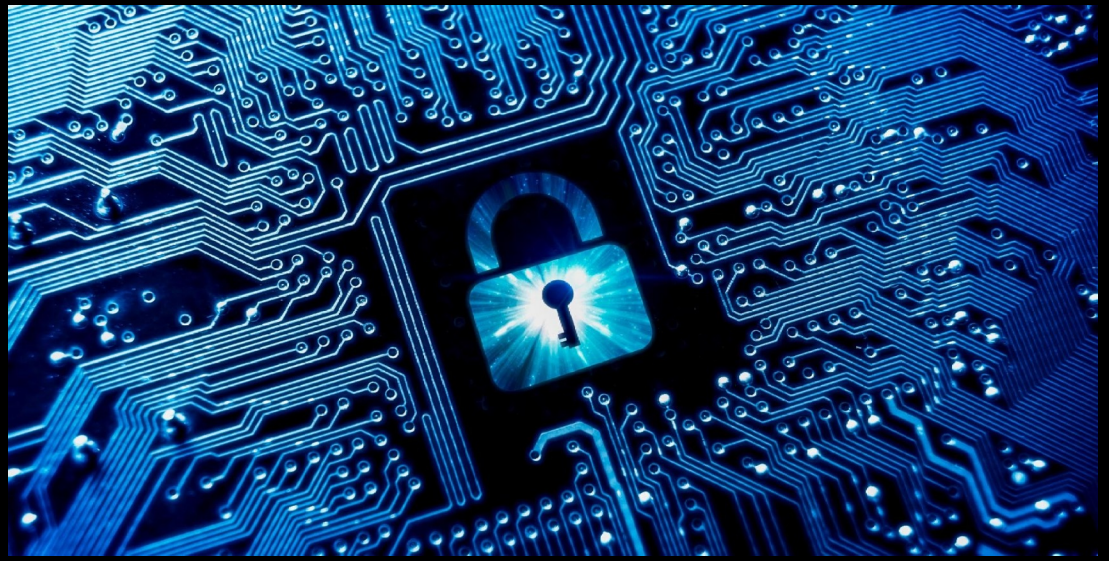
McAfee™

CYBERCITY
CONFERENCE 10.01.19

Solutions?

Strong (Design) Principles

- ✓ Info-Sec
- ✓ IT-Ops
- ✓ Dev-Ops



1. No Hardcoded Secrets

- Plaintext secrets/credentials in source code.
- Seeds for random number/key generation
- Stored value on local system (e.g., registry)
- Static names for IPC, Sync. objects etc.
- May impact the entire ecosystem

Example: Uber Breach (2016)

- Plaintext credentials used in source code
- Access to AWS instance of Uber
- Developer “accidentally” posted on GitHub
- 57M customers + 600,000 drivers’ info exposed

Secrets must be generated dynamically as they’re needed

2. No Known Vulnerabilities in Production

3. No Direct Access to 3rd-party Services

Web Calls Must be Verified

4. No Interface for SQL Queries

5. No CLI into Sensitive Components

6. No Employee Access to Signing Server

7. Access

- ✓ Biometric
- ✓ Multi-factored
- ✓ Deactivation

Miscellaneous

Summary

Insider Attacks

- ✓ Consequences are costly
- ✓ Insiders are everywhere
- ✓ No exhaustive countermeasures
- ✓ Careful design could reduce the attack surface significantly

CYBERCITY
CONFERENCE 10.01.19

McAfee™

THANK YOU

CYBERCITY
CONFERENCE 10.01.19