When Your Firewall is Held Ransom: Best Practices to Thwart Modern Vulnerabilities

CAMPBELL MURRAY
Global Head, Cybersecurity Consulting,
BlackBerry

EMPOWERING THE SECURELY CONNECTED WORKFORCE

BlackBerry® Secure™

WORLD TOUR

Agenda

The scale of the problem

How to respond to an attack

Preventative measures

Security Engineering

Futurology

1 The scale of the problem

2018 attacks

- **Aadhaar, January 3, 2018**
  - India's giant one billion person public database was been compromised.
  - Former staff members provided access to names, email addresses and phone numbers.

- **Ransomware was the cause of 39% of malware-related data breaches, more than double that of last year.**

- **Estimated costs to business:**
  - $400 billion annually
  - Costs increasing 22.7% every year
  - Breaches increasing by 27.4% every year
  - Average cost per breach $11.7M

Despite everything we have learned, the outcomes are escalating.

Source: Accenture

2 So what do you do when it happens to you?

How to respond to an attack:

Incident response

Messaging tree

- Standards e.g ISO 27001

Public messaging and PR

Legal

Forensics

- Triage and investigation.

Lessons learned

- What should you be taking away from a breach?

How do you prevent this happening at all?

Device management Patching

- Resource issues
- Diversity in technology and devices
- Remote working, BYOD and IoT compound the problem

Identifying vulnerabilities

- Threat surface management
- Threat intelligence

Wet Ware – staff are the weakest link

- Social engineering
- Employees - Aadhaar

DDPRR

- Deter
- Detect
- Protect
- React
- Recover

Principals of security engineering

SSDLC

- Secure Software Development Lifecycle

Errors in code statistics

- 100,000,000 LOC in a Vehicle
- 0.015 defects per LOC = 1,500,000 defects in a Vehicle

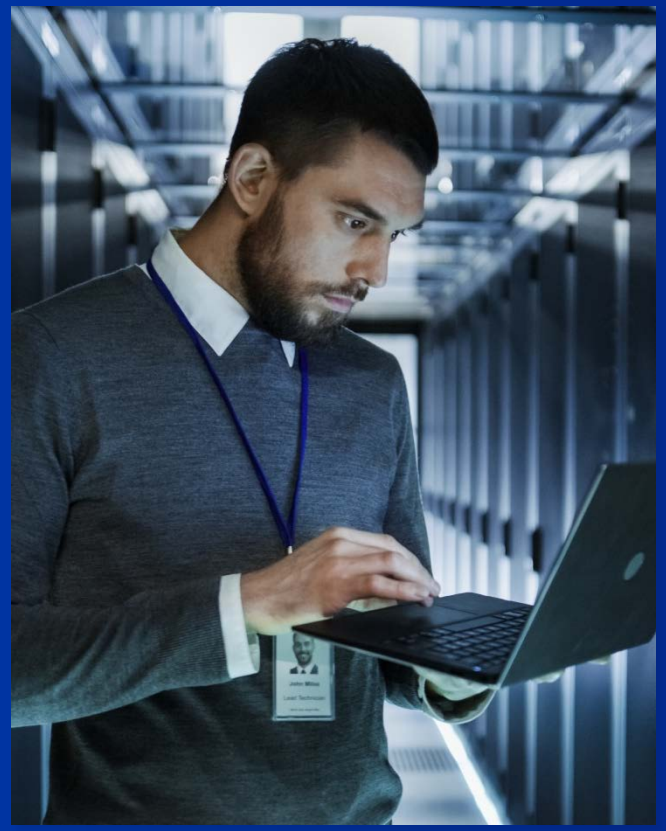
Principals of SCADA / IoT security

- Tenets of SCADA security

The future and security challenges

- IoT and SCADA
- Enterprise of things

Principals of security engineering



Even the most secure organizations find issues:

1008 **Critical**

198 **Severe**

327 **Moderate**

63 **Low**

21 **Public facing documents** (advisories, bulletins)


#BBSWT