Security in the IT and Operational Technology Convergence

Christopher Odutola
Sales Engineer
August 2020
Agenda

• 2019 Review of threats – East Africa
• Overview of IT/OT Convergence
• The Trust factor
• Cybersecurity-as-a-System
• Holistic Cybersecurity Approach
• Conclusion
There is no technology today that cannot be defeated by social engineering

Frank Abagnale, security consultant
Percentage of organizations with cloud account credentials stolen in the last year

Has your organization suffered a public cloud security incident in the last 12 months? “Yes, Stolen Credentials”. Base 3,521 respondents
IT/OT Convergence in a nutshell

The integration of information technology (IT) systems with operational technology (OT) systems

IT systems are used for data-centric computing. OT systems enhance manufacturing and industrial operations e.g. SCADA

IT/OT fusion enables more direct control and more complete monitoring, with easier analysis of data, from anywhere in the world
ICSs, Remote Devices & Vehicles

Cloud and SaaS Apps
- slack
- Dropbox Business
- GoToMeeting
- Office 365
- Salesforce

Corporate HQ
XG 750

Internet and Broadband Services
- 3G/4G/DSL/Cable
- SD-WAN Overlay
- Layer 2 VPN

Sophos Central
Cloud Management and Orchestration

IP Security
- Anti-malware
- IPS
- Secure wireless
- Synchronized Security
- Synchronized App Control

IPv6 and IPv4 Support
- Visitors
- Employees

Segmented Wi-Fi
- APX Wireless
- XG 135

IoT Devices
- Remote terminal units, programmable logic controllers, cameras, etc.

VPN
- Secure wireless
- Zero-touch deployment

Segmented Wi-Fi
- Employees
- Customers

IoT Devices
Digital signage/video displays, cameras, etc.
Digital Transformation (DT) - Cybersecurity

- Cloud is everything
- Internet of Things
- Software as a Service
- Analytics is new Engine
- Data is new Gold
Cloud Security is a Shared Responsibility

Security IN the Cloud
- Host Security
- WAF
- IPS
- VPN
- Next-Gen Firewall
- Outbound Proxy

Applications and Content
- Network Security
- Inventory Configuration
- Access Controls
- Data Security

Security OF the Cloud
- Foundational Services
- Compute
- Network
- Storage
- Availability Zones

Your Responsibility

Cloud Provider Responsibility
- AWS, Azure, Google
Is SSL Inspection Incredibly Important to IT/OT?

Concerning SSL/TLS Trends and Their Impact

Visibility
- Google
- 80% of traffic is Encrypted
- An Enormous Blind Spot

Threats
- SophosLabs
- 32% Malware and PUA connections are TLS
- Hackers are Exploiting it

Performance
- 96% NOT using SSL Inspection
- Organizations are Powerless
Companies need to take a multi-layered approach to data security, from embracing cloud shared security responsibilities and adopting a zero trust model...

Frank Dickson, Program VP, Cybersecurity Products at IDC
Perimeter is changing!

Remote Users

SaaS

aws

Public Cloud / IaaS

TRUSTED

salesforce
Principles of Zero Trust

Trust Nothing, Verify Everything

**Always Identify**
Secure access to all data and resources by user with MFA

**Always Control**
Adopt *Least Privilege* model to enforce access control and segment all workflows

**Always Analyze**
Inspect and record all activity and regularly analyze

**Always Secure**
‘Inside Out’ cybersecurity focused on data and risk
Cybersecurity as a System – Synchronized Security

**ANALYZE**
- Discover users, apps, devices, and data – on-prem, and in cloud
- Identify and authenticate in real-time

**ADAPT**
- Dynamic security policies based on threat detection, user behavior, traffic analysis, compliance guidelines

**AUTOMATE**
- Network and Wi-Fi access control
- Automatic device isolation
- Traffic bandwidth optimization
Embracing change and getting ahead of the curve is the best prescription to be in control of your organization's destiny and avoid being caught off guard.

Michael Suby, Research VP, IDC Security and Trust
Holistic Cybersecurity Approach

Cybersecurity Model

Cybersecurity System

Synchronized Security

24/7 Threat Hunting/Response