Security in the IT and Operational Technology Convergence

Christopher Odutola
Sales Engineer, West Africa

August 2020
Agenda

• 2019 Review of threats – West 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

Cost Savings

- Work faster
- Do more with less
- Stay ahead
ICSs, Remote Devices & Vehicles

- Cloud and SaaS Apps
- Corporate HQ
- Internet and Broadband Services - 3G/4G/DSL/Cable
  - SD-WAN Overlay
  - Layer 2 VPN

- Segmentated Wi-Fi
  - APX Wireless
  - XG 135

- IoT Devices
  - Digital signage/video displays, cameras, etc.

- Sophos Central
  - Cloud Management and Orchestration

- Sophos XG 750

- Segmentated Wi-Fi
  - Employees
  - Customers

- SD-RED 15w

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

- Employees
- Visitors

- SOPHOS

- Internet
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

<table>
<thead>
<tr>
<th>Security in the Cloud</th>
<th>Your Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Security</td>
<td>WAF</td>
</tr>
<tr>
<td>Applications and Content</td>
<td></td>
</tr>
<tr>
<td>Network Security</td>
<td>Inventory Configuration</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security of the Cloud</th>
<th>Cloud Provider Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foundational Services</td>
<td>AWS, Azure, Google</td>
</tr>
<tr>
<td>Compute</td>
<td>Network</td>
</tr>
</tbody>
</table>
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

aws
Public Cloud / IaaS
SaaS

TRUSTED
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

Cloud Computing Instances

Users

SaaS Applications

Devices

Firewall  Wireless  Email  Web  Sophos Central  Encryption  Mobile  Server  Endpoint

Mobile Encryption Server

Web Wireless Email

Endpoint

SaaS Applications
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

Synchronized Security

Cybersecurity Model

Cybersecurity System

24/7 Threat Hunting/Response