Securing the business in the digital era

Sujata Ramamoorthy
Director, Cloud Platform Security
September 14, 2017
Agenda

- The digital world
- Security landscape
- Cloud trends and challenges
- Cisco practices – Cloud, data and threats
- Summary
An irreversible digital economy

The digital economy and technology are interconnected

- Hyper connectivity
- Unlimited computing power
- Cloud computing
- Mobile computing
- Continuous stream and access to information
- Pervasive cybersecurity and regulations

Source: IDC 2016
Fitness going digital from active wear to digital coaching

Active monitoring (big data apps)

MapMyFitness

Endomondo

MyFitnessPal

Big data

“The world’s most valuable resource is no longer oil, but Data”
– The Economist, May 2017
Living in the cloud
Companies today are born digital
The global digital economy has come of age
An era of rapid change
Threat landscape
Exploit kits fade into the shadows
Adversaries focus on other attacks
DDoS
Botnets compete to control IoT and have the ability to clog up the Internet

- IoT DDoS attacks propelled us into the 1TBps DDoS era
- Set up can be completed within an hour
- Distribution is rapid. Perpetrators can have a botnet of 100,000+ infected devices in 24 hours
- The malware has a low detection rate. It is very difficult to retrieve samples because the malicious code lives in the device’s memory and is wiped out once the device is restarted

Source: Radware
Business email compromise
Social engineering problem that could be bigger than ransomware

Ransomware

$1B
2016

Business email compromise

$5.3B

Source: Flashpoint
Emerging ransomware tactics

- Using ransomware codebases to their advantage
- Ransomware-as-a-Service (RaaS) platforms are growing fast
- Ransom Denial of Service (RDoS)
Dark cloud

As cloud systems become more leveraged in the organizations, it also presents a new level of risk for security teams.

- Cloud apps expand rapidly in organizations
- Millions of employees leverage cloud apps
- The app risk levels are rising
- OAuth grants access to organization backbone
- Excessive number of privileged users
- Percentage of DevOps servers left wide open are creating a huge ransomware risk

Adversaries

- Target privileged users to steal credentials
- Access to the entire network
- Leverage previously breached credentials
Cloud trends
The trend toward cloud

95% of Respondents are using cloud

Public cloud only: 22%
Private cloud only: 5%
Hybrid: 67%

Public = 89%
Private = 72%

Source: RightScape 2017 State of the Cloud Report
Enterprises rating cloud security as a significant challenge

- 2015: 41%
- 2016: 37%
- 2017: 35%

Source: RightScale 2017 State of the Cloud Report
Cisco’s growing cloud presence
Digitization fundamentally changes security landscape

- Speed of business
- New richer targets
- Emergence of cybercrime as-a-service
- Increased impact/loss
Cisco Security practices

Cloud

Data

Threat detection/ containment
Cloud Security
Security responsibilities
Cloud providers vs. consumers

Application
Platform architecture
Virtualized infrastructure
Hardware
Facility

Consumer
IaaS
PaaS
SaaS

Provider
IaaS
PaaS
SaaS
What is the providers role?
Cloud security models will leverage…

- Encryption and key management
- Event monitoring
- Security features, automation
- Transparency
- Segmentation
- Strong authentication

Cloud architectures
What is the consumer’s role?

Policy  
Engagement  
Monitoring  
Integration
Security of the procured Cloud Services
(Cloud assessment and service provider remediation)

- Privacy & data security
- Application security
- Infrastructure security
- Authentication & authorization
- Vulnerability management
- Logging & auditability
- Support & operations
- Incident analysis & response
- Business continuity

CASPR Models
- Restricted
- Highly confidential
- Confidential
- Public
Security in our cloud offers
Model to drive trust

Build
- Security standards and architectures
- Threat analysis and protection
- Quality management
- Common secure services

Operate
- Data encryption and protection
- Assessment activities
- Intrusion detection and prevention systems
- Security governance

Monitor
- Policy and compliance
- Transparency to enable customers
- Secure cloud value chain
- Application layer data and event monitoring
Data protection
Key elements of a data protection program

- Policy, standards and taxonomy
- Identification and classification
- Data risk and organizational maturity
- Awareness and education
- Oversight and enforcement
- Privacy and international privacy policy
- Security and data loss prevention
- Incident management

Foundational
Preparing for General Data Protection Regulation (GDPR) – May 2018

- Policy and process updates
- Data inventory/risk assessments
- Data impact assessments
- Vendor management
Threat detection and response
Integrated threat defense

13 iPOPs globally

AMP’d web and email
- 1% of all WSA transactions blocked
- 80 WSAs/30 ESA Deployed
- 3K+ email files blocked by AMP monthly

Threat Grid/AMP
- On-Prem sandboxing
- 10K+ files analyzed every 24hrs.
- 14 TG appliances deployed

Cloud Enabled AMP

AMP for Networks
- Passive and inline capabilities
- 25K+ quarterly alerts and VM series deployed
- NG-IPS 83xx

AMP for Endpoints
- Machine learning engine
- 10K+ agents deployed
- Analytics engine

FireSIGHT Management Center
- Eight global appliances deployed
Expecting the unexpected
Incident detection and containment – circa 2017

Integrated protection – advanced correlation
47TB Traffic inspected p/day * 1.2T Events monitored * 14 Incidents p/day
Information Sharing

What are we trying to protect?
Collect/Analyze

1.2T events throughout network
47TB traffic inspected
15B NetFlows analyzed/day
Active directory servers
4TB data collected and analyzed
~200 Plays
End user laptop

What are the threats?

DoS attack
SQL Injection
Directory traversal
Network lateral movement
Account compromise
Malware
Malware
Phishing attacks
Drive-by download

How do we detect them?

NetFlow monitoring
IPS/IDS detection
System logs
User activity
HIPS logs
HIPS/AV logs
ESA logs
WSA logs

How do we respond?

Engage ISP
Investigate
Mitigate P1 incident
Investigate
Remediate
Reimage
Investigate
### Actionable steps to sleep better at night

<table>
<thead>
<tr>
<th>Get educated</th>
<th>Overwhelmed defenders</th>
<th>Executive leadership</th>
<th>Balance defense with active response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business landscape, threat landscape, security programs and what you can do better continuously</td>
<td>Simplify, integrate, automate (vendors, solutions)</td>
<td>Engage early on (IT/OT, risk/ rewards, fiscal impact, budget, train personnel)</td>
<td>Don’t set and forget, establish business continuity/disaster recovery plan</td>
</tr>
</tbody>
</table>