Cloud and Critical Infrastructures: how Cloud services are factored in from a risk perspective

Reaching the Cloud era in the EU
Riga 16 June 2015

Jonathan Sage
Government and Regulatory Affairs
Cyber Security Policy Lead, Europe
Today’s conversation.

• **Current and emerging attacks and incidents**

• **Changing approaches and addressing security - risks relating to Cloud**

• **Collaboration - Incident Sharing / Information Sharing (privacy, liability)**

• **Emerging Regulation on the Horizon (critical, reporting, risk, standards)**
Organizations today face a growing range of cyber adversaries…

- The number and variety of new adversaries and threats continues to grow
- Old threats don’t always disappear – while new threats continue to add to the total landscape
An evolving landscape, how many events, attacks and incidents, what the average finance organization is looking like.

**Security events**
- **Annual**: 61,126,420
- **Monthly**: 5,260,535
- **Weekly**: 1,213,969

**Security attacks**
- **Annual**: 13,673
- **Monthly**: 1,139
- **Weekly**: 262

**Security incidents**
- **Annual**: 126
- **Monthly**: 10
- **Weekly**: 2.41

- **Security Intelligence**
  - Correlation and analytics tools
  - Human security analysts

**Events: Increased efficiencies in tuning year on year to 61m**
- Observable occurrences in a system or network

**Attacks: Increased efficiencies achieved decreased attack volume**
- More efficiency in security processing to help clients focus on identified malicious events

**Incidents: up 8% year on year**
- Attacks deemed worthy of deeper investigation

Source: IBM Cyber Security Index 2015
An increasing amount of feeds to ingest, a challenge to reach prioritized data that optimizes threat prevention and response

**Internal**

- Threats and exposures that affect a specific organization

- **Firewall logs**
- **Proxy logs**
- **IDS/IPS logs**
- **Endpoint security logs**
- **Employee directory**
- **Web logs**
- **Application logs**
- **Authentication logs**
- **Malware detection logs**
- **SSO/LDAP context**
- **Network security logs**
- **Building access logs**
- **Fraud payment logs**
- **Application inventory**
- **DNS/DHCP logs**
- **Call/IVR logs**
- **Website marketing analytics**
- **CSIRT incidents**
- **Vulnerability patch mgmt**

**Ever-increasing proliferation of data sources**

**External**

- Third party insight
- Industry- and geography-specific threats and trends

- **Top tier phishing indicators**
- **Brand abuse phishing indicators**
- **Malware campaigns/indicators**
- **Fraud payment logs**
- **Actor intel/indicators**
- **Staff asset/credentials**
- **Customer assets/credentials**
- **Threat landscape intel**
- **Intel as a service (IaaS)**
- **Human intel (HUMINT)**
- **Law enforcement threat intel**
- **Industry threat intel sharing**
- **Public sector threat intel**
- **ISAC threat intel**
- **Technical intel (TECHINT)**
- **IP reputation intel**
- **Passive DNS intel**
- **OSINT sentiment analysis**
- **Underground/Dark Web intel**
- **Malware Hashes / MDS**

---

1. Intrusion detection system / intrusion prevention system (IDS/IPS); Single sign-on (SSO) / lightweight directory access protocol (LDAP); 2. Computer security incident response team (CSIRT); 3. Domain name system (DNS) / dynamic host configuration protocol (DHCP); 4. Interactive voice response (IVR); 5. Information sharing and analysis center; 6. Intellectual property; 7. Open source intelligence (OSI); 8. Malware detection or defense system (MDS)

© 2015 IBM Corporation
Cloud plays many different roles – emergence of HYBRID

- Not critical per se, cloud is becoming increasingly deployed everywhere in the IT landscape
- Not all cloud is PUBLIC
- Risk based approach
- Need to look at how cloud is deployed and secure appropriately

#1 concerns for cloud are security and privacy*

* Source: Gartner
Cloud is not inherently more risky than traditional IT

- Not everything is critical – depends on for what purpose cloud is used
- Problems facing cloud providers in an enterprise environment if they have to report an incident out to another authority
- Causes conflict between cloud user (data controller) and cloud provider (data processor)

* Source: Gartner
The changing approaches...current and emerging

- Prepared - taken appropriate steps.
  - Governance as well as technical

- Assurance - risk assessment and testing
  - Threat based intelligence integrated

- Detection and Response
  - Able to capture / report critical incident
  - Having the data / Recognizing the incident.

- Information sharing exchanges
  - Advancing protection – automated real time digesting
  - Addressing liability issues and Maintaining privacy
Thank you