Session 3: Cyber-criminality, security and risk in an IoT world

Belisario Contreras
October 2017
The opinions expressed in this presentation do not necessarily reflect the views of the General Secretariat of the Organization of American States or the governments of its member states.
How will IoT change the future of cybercrime and how is it being addressed?

- Absence of security protocols related to IoTs makes them easy targets for data mining.
- IoT are now hyper connected and expands the sources of data that law enforcement will need access to.
- Ease of use for users = Ease of access for attackers (e.g. webcams default settings).
- Privacy vs Public Safety concerns.
Threats

IoT mostly consists of systems or services traditionally called “M2M” (Machine to Machine) e.g. smart meters connected to national grids

Application platforms built operating systems that have exploitable vulnerabilities

Criminal activities could involve disruption of services such as traffic control systems or public transportation systems
Advances in legislation

Most countries have no laws that specifically mention IoT devices, so general privacy laws would apply.

European Commission draft ePrivacy Regulation of IoT:

“In order to ensure full protection of the rights to privacy and confidentiality of communications, and to promote a trusted and secure Internet of Things in the digital single market, it is necessary to clarify that this Regulation should apply to the transmission of machine-to-machine communications. Therefore, the principle of confidentiality enshrined in this Regulation should also apply to the transmission of machine-to-machine communications.”
Advances in legislation

In Canada, a federal law called the **Personal Information Protection and Electronic Documents Act** (PIPEDA) sets rules on how companies who collect personal data should protect it. The law requires companies to do things like create a privacy management program, limit collection, use and retention of data, give users access to information that the company has about them and provide a way for users to file complaints with the company.

In the USA, according to the **National Conference of State Legislatures** website, 31 states have data disposal laws and 47 states have security breach notification laws, but the laws are not uniform.
Conversion of IT, Operations Technology and IoT

A recent example is the Target case, where a cybercriminal was able to install malware into numerous company point-of-sales terminals by first gaining entry through a vulnerability in the company’s IoT HVAC system.
Colombia (2011 & 2016)

Jamaica 2013

Panama 2013

Trinidad and Tobago 2013

Paraguay 2017

Chile 2017
National Strategies under development

Costa Rica
Argentina
Dominican Republic
Guatemala
Mexico
Peru
New Requests of Assistance

Honduras  Belize  Barbados
Cybersecurity: Are we ready in Latin America and the Caribbean?
<table>
<thead>
<tr>
<th>Country</th>
<th>Policy and Strategy</th>
<th>Culture and Society</th>
<th>Education</th>
<th>Legal Frameworks</th>
<th>Technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Argentina</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Brazil</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chile</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Colombia</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mexico</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Uruguay</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Challenges in the region

18 countries have NOT identified “key elements” of their National Critical Infrastructure

28 of 32 countries do not have cyber security strategies

24 do not count with mechanism for planning and coordination on Critical Infrastructure Issues
Challenges in the region

In 20 countries no command and control center exist, and in another 7 this function is performed without formality.

26 countries in the region do not have a structured cybersecurity education program.

In 30 of the 32 countries, there is no national cyber security awareness programs.
Current Overview of CSIRTs in the Region
National CSIRTs
(2017) estado actual

- ICIC CERT
- CCIRC
- US-CERT
- CTIRGov
- CERT-MX
- CSIRT GOB CL
- CL-CERT
- ADSIB
- CSIRTGt
- PE-CERT
- SurCSIRT
- EcuCERT
- ColCert
- CSIRT-GY
- TT-CSIRT
- JM-CSIRT
- VenCERT
- CERT-PY
- CERTUy
- CSIRT Costa Rica
- CSIRT Panama
CSIRTAmericas.org
Hemispheric Network
Consolidating an Operational Community in the Americas

Encourage the exchange of alerts and information
+ 65
Procedures, scripts, manuals sharing between CSIRTs

+ 3000
Monthly alerts are notified to CSIRTs in the region

Large scale incident coordination operations (WannaCry / Petya / nopetya)

Subregional trends every 6 hours
North, Central, South, Caribbean

CSIRTs
55 members

Argentina
Bolivia
Chile
Mexico
Trinidad and Tobago
Colombia
Guyana
Venezuela
Suriname
Paraguay
Jamaica
Panama
Costa Rica
Ecuador
Peru
Argentina
Thank you!
Merci
Gracias
Obrigado

Belisario Contreras

Cybersecurity Program
Organization of American States
cybersecurity@oas.org
@OEA_Cyber