Securitatea Cibernetică în Aviație

Prezintă: Daniel Ester

romatsa

romanian air traffic services adminstration

La ce se referă:

- Securitatea cibernetica se referă la prevenirea și/sau reacția la acte intenționate desfășurate în spațiul cibernetic pentru compromiterea directă a sistemelor sau pentru împiedicarea funcționării sistemelor de protecție.
- Spațiul cibernetic se referă la domeniul schimbului de informații între sisteme și rețele de calculatoare și include atât sisteme fizice cât și resurse virtuale.
- Securitatea cibernetică în domeniul aeroportuar și a managementului traficului aerian are ca scop limitarea efectelor acestor amenințări asupra operării normale.

Cadrul de reglementare

- Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice a intrat în vigoare de la 12 ianuarie 2019.
- Legea transpune așa-numita Directivă NIS (Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune) .
- Inițiativa Single European Sky prin “Single European Sky ATM Research Joint Undertaking” – “SESARJU”
- Regulamentul European pentru protecția datelor personale - GDPR

Proiecte la nivel European privind securitatea cibernetică in aviație

- A fost publicat raportul final **“Addressing Airport Security”**

- Este în derulare proiectul “SWIM common PKI and policies and procedures for establishing a Trust Framework” la care este participant și ROMATSA.

Proiectul are ca scop implementarea unei infrastructuri digitale la nivel European (în aviație) având ca scop utilizarea de chei digitale pentru autentificarea sistemelor și securizarea comunicației între acestea.

Proiecte la nivel European privind securitatea cibernetică in aviație

- **Proiectul European "Network Management Cybersecurity"**

Se vor implementa următoarele îmbunătățiri la nivelul sistemelor curente:

- **Sistem de Management al Securitatii Informatiei - Information Security Management System (ISMS):** Implementarea unui ISMS va necesita definirea politicilor, evaluarea riscurilor, stabilirea procedurilor și uneltelor de monitorizare
- **Centrul de operare a securității - Security Operations Centre (SOC)**

Contextul Securității Cibernetice:

- Sisteme de calcul puternice și foarte complexe;
- Legături de comunicație foarte rapide;
- Sisteme puternic interconectate;
- Apariția “Internet of Things” (IoT) si retelelor 5G (viteze de comunicatie de ordinal 10Gb – 50 Gb).

Principalele amenințări cibernetice nu sunt sub controlul nostru:

1. Atacuri conduse/sponsorizate la nivel statal

Sunt extrem de sofisticate si nu pot fi evitate in context politic tensionat.

2. Criminalitatea cibernetică

A devenit o industrie.

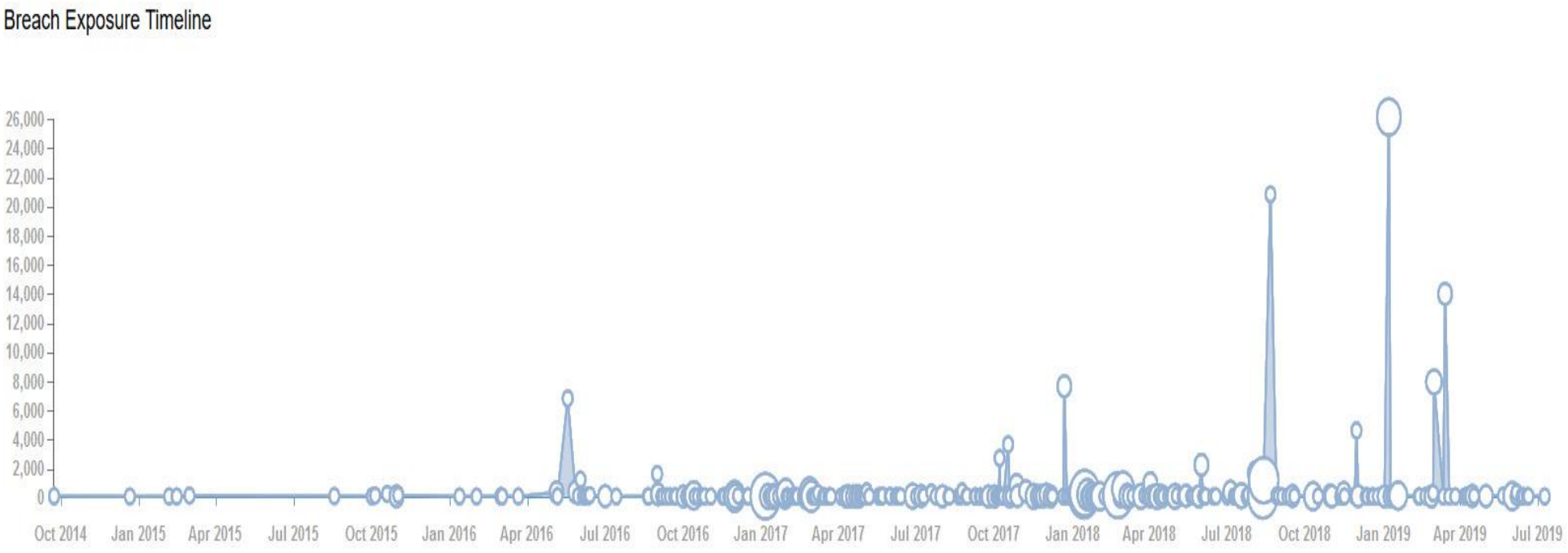
Acționează prin grupuri organizate, puternice și cu mare calificare.

3. Hacktivism (uneori cu motivări privind conservarea mediului)

Unele grupări au țintit deja aviația și o vor face și în viitor deoarece percep impactul acesteia ca fiind negativ asupra climatului.

Puterea acestor grupări o reprezintă motivația, dispun de o rețea de specialiști calificați.

Riscul de securitate cibernetică evoluează cu o dinamică ridicată



Abordarea izolaționistă nu este o soluție deoarece:

1. Participanții în industria aviației sunt inter-conectați;

2. Atacurile pot veni prin intermediul unui participant din industrie, nu numai din exteriorul infrastructurii;

3. Este necesară anticiparea atacurilor cibernetice și pregătirea pentru acestea în vederea reducerii riscurilor.

Soluții:

1. Investiția în resurse umane:

- Schimbarea modului de gândire la nivel de management;
- Educarea întregului personal privind măsurile de securitate cibernetică.

2. Adaptarea proceselor prin:

Implementarea unui sistem de gestiune a securitatii aliniat cu alte sisteme de management.

(vezi EASA NPA 2019-07 “Management of Information Security Risks”)

Soluții:

3. Utilizarea unor mijloace de dezvoltare a sistemelor ce țin cont de aspecte de securitate;

4. Implementarea unui “cadru de încredere” prin:
   - Utilizarea cadrului de reglementare cibernetică din cadrul EASA;
   - Partajarea informațiilor legate de incidente de securitate;
   - Coordonarea crizelor/incidentelor la nivel pan-european;

Soluții:

5. Implementarea unui centru de operații de securitate – SOC sau echivalent avand ca scopuri:
   - Evidența clară a componentelor dintr-o rețea
   - Prevenirea atacurilor
   - Gestiunea alarmelor
   - Detecția rapidă a atacurilor
   - Conștientizarea contextului
   - Răspunsul la incident
   - Revenirea la operarea normală

Aspecte importante privind construcția/operarea unui Centru de operare a securității - SOC

1. Personalul

   Personalul calificat în securitatea cibernetică este limitat și foarte cerut pe piața forței de muncă.

2. Proiectarea centrului de operațiuni

   Utilizarea platformelor de securitate este dependentă de nivelul de expertiză al personalului.

   Nu este indicată fluctuația de personal.

Aspecte importante privind constructia/operarea unui SOC

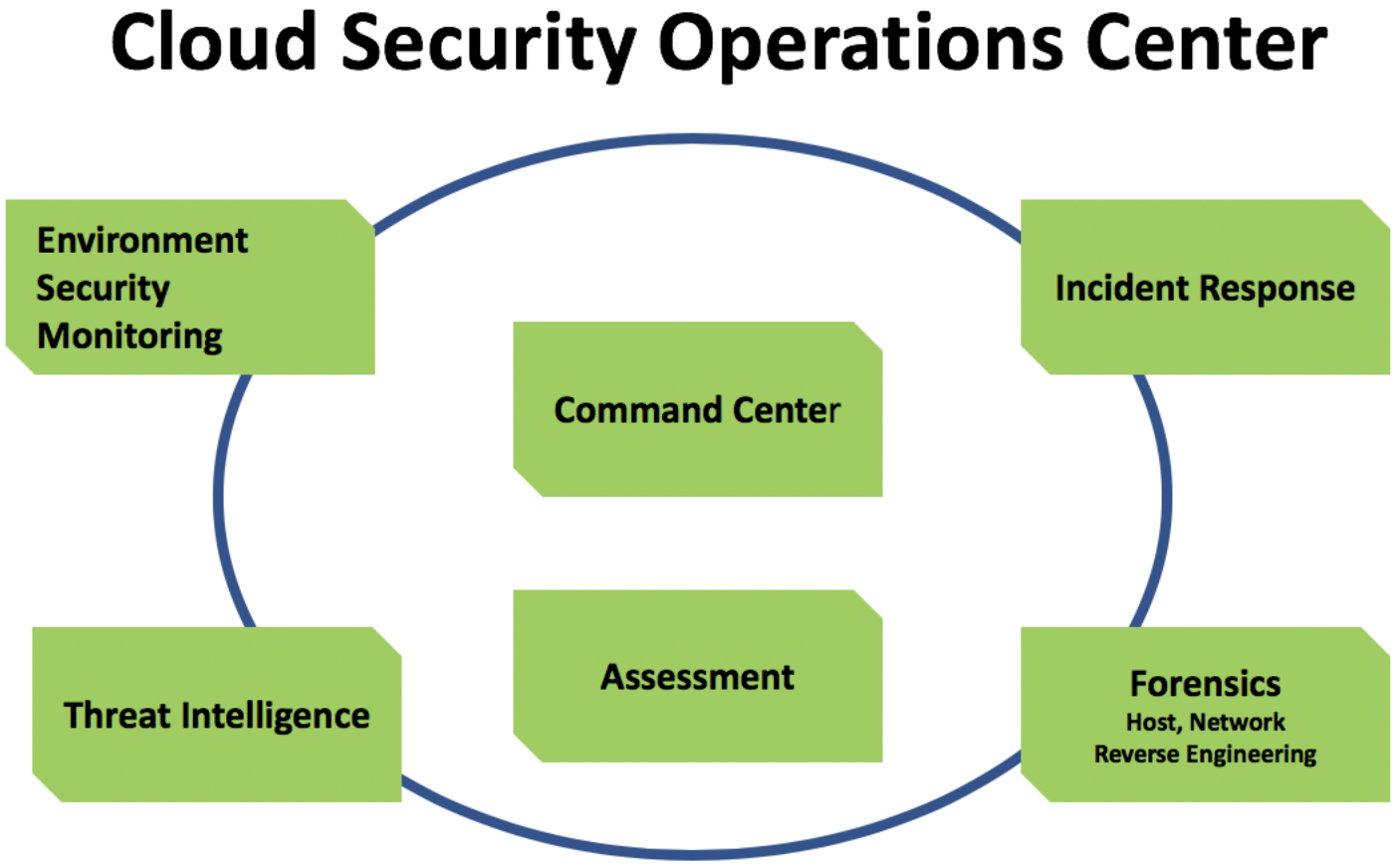
3. Detecția amenințărilor interne

   Echipamentele utilizate în detecția atacurilor furnizează informații privind activitatea infrastructurii.

4. Trebuie să se dispună de informații privind tipurile de atac.

5. Analiza datelor este un element cheie.

SOC


Cloud Security Operations Center
Environment Security Monitoring
Incident Response
Command Center
Assessment
Threat Intelligence
Forensics
Host, Network
Reverse Engineering

Aspecte privind resursele umane:

- De cele mai multe ori echipele de securitate cibernetica sunt sub-dimensionate
- Echipele de securitate nu au vizibilitate suficientă pentru a discerne ce se întamplă

Echipa SOC trebuie să aibe cunoștințele adecvate, să utilizeze corect resursele disponibile și să aibe vizibilitate asupra amenințărilor active sau viitoare.

Analiștii de securitate se pot organiza pe mai multe categorii de activitați:

- Trierea evenimentelor
- Răspunsul la incident
- “vânătorul de amenințări”
- Șeful operațiunilor de conducere a SOC

Despre procese/proceduri privind evenimente de securitate:

1. Clasificarea și trierea evenimentelor;
2. Prioritizare și analiza a evenimentelor;
3. Remedierea și recuperarea în caz de incident;
4. Evaluare și audit.

Unelte utilizate in SOC

1. Inventarul sistemelor;
2. Evaluarea vulnerabilităților prin utilizarea de unelte adecvate;
3. Monitorizare comportament;
4. Detecția intruziunilor;
5. Gestiunea evenimentelor și informațiilor privind securitatea = SIEM

Analiza evenimentelor de securitate trebuie să țină cont de :

- Contextul unui atac
- Cui i se poate atribui un atac
- Asigurarea unui răspuns rapid și eficient

Lecții din lumea reală:

1. Trebuie să fim informați și nu depășiți;

2. Trebuie să dispunem de o rețea de ajutor în caz de incident;

3. Trebuie să avem la dispoziție o platforma unificată de gestiune a incidentelor de securitate

Dificultăti reale privind implementarea SOC în aviație:

- Sisteme autorizate la care este greu de făcut audit de securitate în timpul operării;
- Sisteme autorizate la care este greu de menținut la zi software-ul privind incidentele de securitate;
- Aplicații specifice, “exotice” pentru piața obisnuită a furnizorilor de securitate.

Mulțumesc!