Considerente privind securitatea fizică și cibernetică în domeniul aeroportuar

RASIROM

Protejăm ceea ce contează

- prin tehnologie -

www.rasirom.ro

“Într-o eră a globalizării, ameninţările îndepărtate pot constitui o ameninţare în aceeaşi măsură cu cele apropiate…”

(Strategia Europeană de Securitate)

“Putem ignora realitatea, dar nu putem ignora consecințele ignorării realității.”

(Ayn Rand)

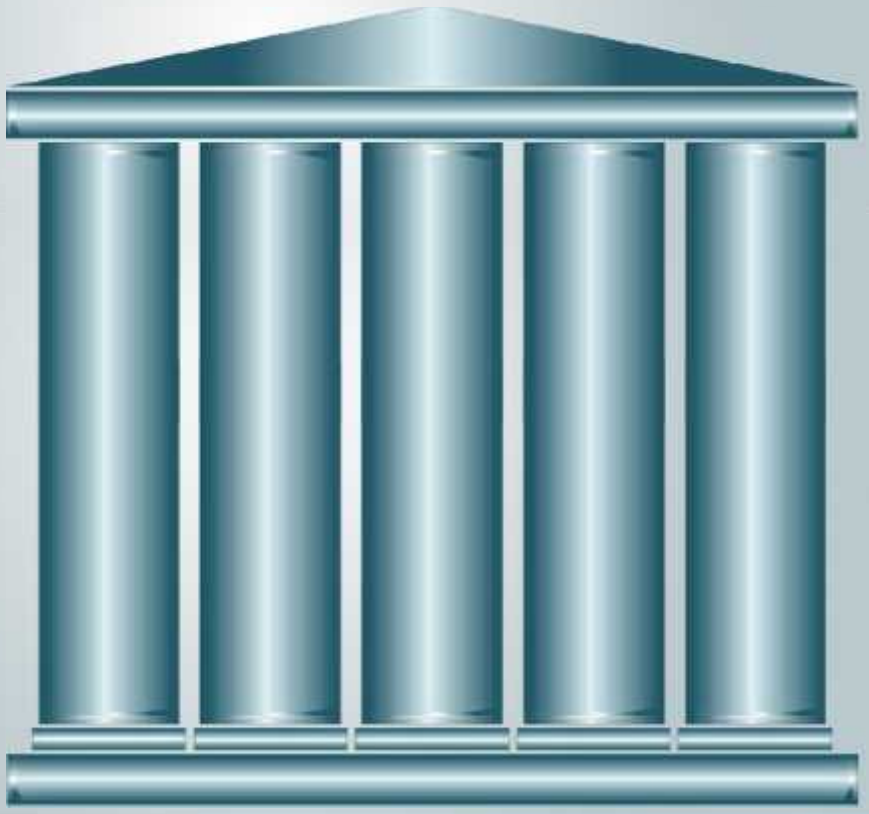
Protejarea unui obiectiv încadrat în categoria infrastructurilor critice

”Protecţie” înseamnă orice activitate care are drept scop asigurarea funcţionalităţii, a continuităţii şi a integrităţii infrastructurilor critice pentru a descuraja, diminua şi neutraliza o ameninţare, un risc sau un punct vulnerabil.

Obiectivul care se încadrează în categoria infrastructurilor critice necesită instalarea următoarelor sisteme:

Spaţiul cibernetic se caracterizează prin lipsa frontierelor, dinamism şi anonimat, generând deopotrivă oportunităţi de dezvoltare a societăţii informaţionale bazate pe cunoaştere, dar şi riscuri la adresa funcţionării acesteia -la nivel individual, statal şi chiar cu manifestare transfrontalieră.

Buna guvernanţă cibernetică reprezintă o activitate complexă, multilaterală şi multi-nivel.



Se fundamentează pe 5 piloni principali:

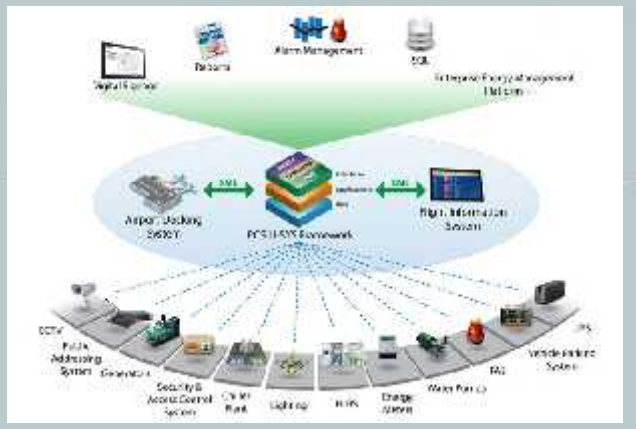
- cadru legislativ flexibil – esenţial pentru managementul provocărilor la nivel cibernetic;
- instrumente tehnice robuste – în suportul sistemelor de avertizare timpurie, contracarare şi reziliență;
- structură organizaţională adaptabilă –esenţială pentru maximizarea eficienţei conlucrării dintre actorii direct interesaţi;
- dezvoltare continuă;
- cooperare internaţională.

Asigurarea securității cibernetice a rețelelor informatice care guvernează activitatea aeroportuară

Rețele de business

Rețele pentru rezervări

Rețele operaționale



Planifică **Construiește** **Supraveghează** **Detectează** **Răspunde** **Raportează** **Îmbunătățește**

Atacuri cibernetice asupra aeroporturilor și companiilor aeriene 2015 și 2016

Romania-Insider.com

Daily News | Discover Romania | Experience Romania | Expat Life | Community Voice

DAILY NEWS / BUSINESS

Romania moves from source to target for cyber attacks

Romania has been a source for cyber-attacks to other states in the past years but it may become the target of such attacks in the near future, a favorite target for hackers or cyber criminals, reports local Hotnews.ro.

In 2015, most of the cyber-attacks against Romania came from Russia and China. In general, the cyber-attacks initiated by state actors targeted Romania for its role in international structures such as NATO and the EU, similar events occurring in other member states.

According to experts from the cyber system, the state actors are often hidden behind groups of hackers or criminal networks, and the Internet is not an easy environment to monitor so identifying a state as the source of an attack is difficult.

BBC | Sign in | News | Sport | Weather | Shop | Earth | Travel | More

NEWS

Home | Video | World | UK | Business | Tech | Science | Magazine | Entertainment & Arts

UK | England | N Ireland | Scotland | Wales | Politics

Cyber attacks: Two-thirds of big UK businesses targeted

9 May 2015 | UK

Share

PA

Two-thirds of big UK businesses have been hit by a cyber attack in the past year, according to government research.

Most of the attacks involved viruses, spyware or malware. The Cyber Security Breaches Survey says. A quarter of large firms experiencing a cyber breach did so at least once a month.

Digital Economy Minister Ed Vaizey said it was "absolutely crucial businesses are secure and can protect data".

In some cases the internet-linked attacks cost millions of pounds.

The survey's results have been released alongside the government's Cyber Governance Health Check launched following the TalkTalk cyber attack in October last year.

The phone and broadband provider, which has over four million UK customers, said some of their banking details and personal information could have been accessed in the breach.

In light of these surveys, businesses are now being urged to protect themselves better.

Hacking Attack At Vietnam Airports Another Chapter In South China Sea Dispute

Hackers can hijack aircraft using WiFi network, warns aviation expert

Terrorists could sabotage systems through passengers' phones, expert says during National Security Middle East conference in Abu Dhabi

More than 100 flight delayed due to cyber-attacks at Vietnam's airports

ALERT British Airways computer problem causes delays at multiple airports

September 6th 2016

Sweden issued cyber attack alert

With much of Sweden's air traffic crippled on 4 Nov. 2015, authorities in the Scandinavian country notified NATO of a serious, ongoing cyber attack by a hacker group linked to Russian intelligence.

Phishing Scam Targeted 75 US Airports

Major cyberattack carried out in 2013 by an undisclosed nation-state sought to breach US commercial aviation networks, says Center for Internet Security report.

Media agencies reported news of a cyber attack against the Istanbul Ataturk International Airport, the passport control system at the departure terminal was hit causing many problems at the airport.

Report: Hackers broke into FAA air traffic control systems

Breaches exposed sensitive employee data, forced the shutdown of part of a network, and could have allowed hackers to disrupt the agency's mission-critical air traffic network, a government report says.

FAKE BOARDING PASS APP GETS HACKER INTO FANCY AIRLINE LOUNGES

Hackers Replicate TSA Master Luggage Keys

“The Inside Job” – versiunea cyber

CHILLING EMAIL CHAIN AS THEY PLOTTED CARNAGE

POLICE recovered hundreds of emails sent by Karim, many of which were to al-Awlaki.

■ **JANUARY 25, 2010:** al-Awlaki asked Karim for information on 'limitations and cracks in present airport security systems'.

He said: 'Depending on what your role is and the amount of information you can get your hands on, you might be able to provide us with critical and urgent information and you may be able to play a crucial role...

'This is not a weekend religion. The contract is to sell our souls to Allah. The compensation is the Jannah (paradise).'

■ **JANUARY 29:** Karim replied: 'I have been keeping a low profile by hiding my real religious viewpoints, trimming my beard and not getting too involved with the local Muslim community or any Islamic activities, but leading a life that was really killing me inside.

'I have knowledge about key IT hardware locations which if targeted can bring huge disruption to flights and cause a major financial loss.

'I know two brothers, one who works in baggage handling at Heathrow and another who works in airport security. If there are some serious plans, then I can try to motivate them.'

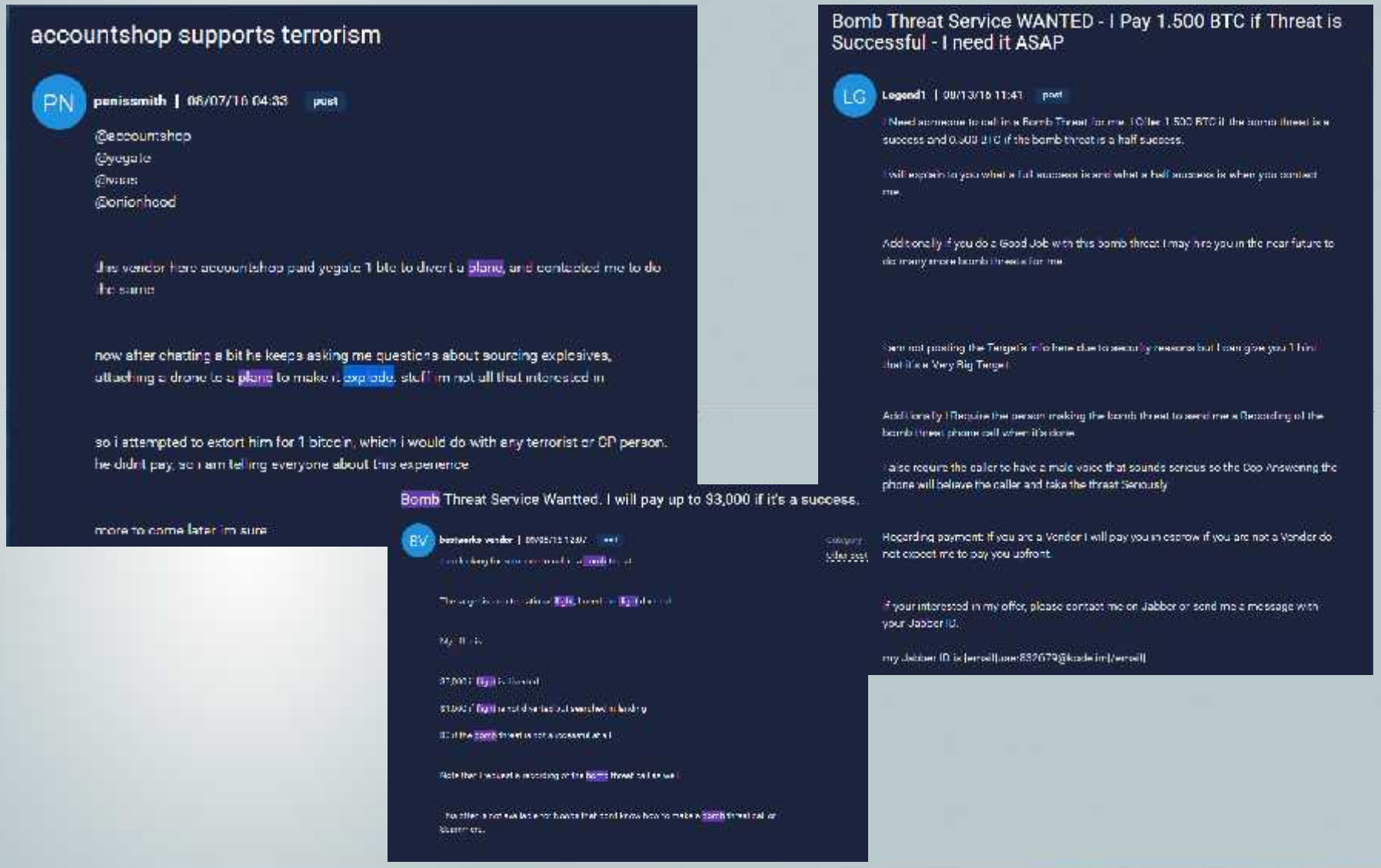
■ **FEBRUARY 13:** al-Awlaki to Karim: 'With the people you have is it possible to get a package or a person with a package on board a flight heading to the U.S?' He added: 'You should definitely take the [cabin crew] opportunity, the information you could get would be very useful.'

■ **FEBRUARY 15:** Karim replied suggesting a cyber attack on BA's website: 'If full damage can be inflicted that would mean cabin crew would be stranded in different parts of the world, planes will be grounded and it will be total chaos.' He added: 'I can work with the bros (brothers) to find out the possibilities of shipping a package to a U.S.-bound plane.'

© PA

Rajib Karim, 31 de ani, un fost expert în computere al British Airways a fost convins să conspire cu un terorist căutat la nivel internațional pentru a plasa o bombă într-un avion.

Aviația în internetul ascuns



Principalele cyber-atacuri aviatice 2015 - 2016

Amenințări cibernetice în aviație

Companie aeriană

- Bază de date nume pasageri
- Detalii financiare
- Istoricul pasagerilor
- Datele zborurilor

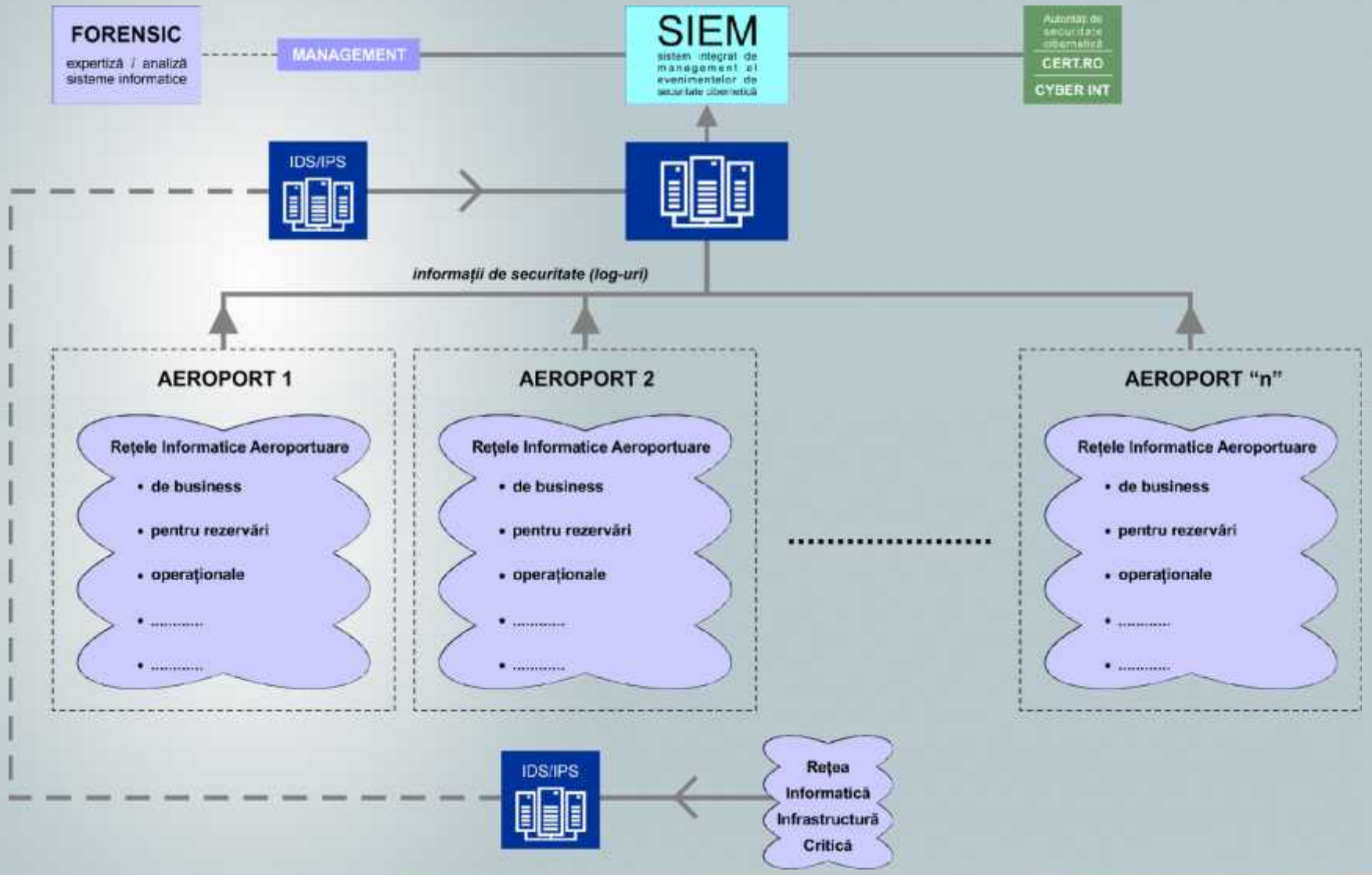
Avion

- Sisteme in-flight
- Thrust Management Computer (TMC)
- Poziție
- Comunicații

Aeroport

- Sisteme de alimentare
- Control pașapoarte
- Sisteme de comunicații
- Sisteme pentru bagaje
- Lanțul de aprovizionare
- Resurse umane

Sistem de securitate cibernetică



RASIROM poate asigura realizarea / implementarea unui astfel de proiect - centru de securitate cibernetică aeroportuară (CERT-AERO) care să aibă următoarele funcționalități CSIRT (Computer Security Incident Response Team):

- Furnizarea de servicii proactive
- Instruirea utilizatorului final
- Răspuns la incidente

Timpul de răspuns constituie un aspect critic în asamblarea, întreținerea și implementarea unui CSIRT eficient. Un răspuns rapid, precis direcționat și eficient poate minimiza daunele de ansamblu ale finanțelor, hardware-ului și software-ului cauzate de un anumit incident.

O altă considerație importantă poate implica abilitatea CSIRT de a urmări autorii unui incident, astfel încât părțile vinovate pot fi închise și urmărite penal în mod eficient.

Un aspect la fel de important îl presupune "rigidizarea" software-ului și a infrastructurii pentru a minimiza numărul de incidente care au loc în timp.

Vă mulțumesc!