Bezbednost informacionih sistema

Tanja Kaurin

Појам и циљеви заштите;
Правни и етички аспекти заштите;
Управљање заштитом;

Злоупотреба информационе технологије

Физичко-технички сегменти заштите;
Организациони сегменти заштите;

Организациони сегменти заштите;
Кадровски сегменти заштите;
Логички сегменти заштите;

Заштита података;
Заштита персоналних рачунара;
Заштита у рачунарским мрежама;

Откривање, разјашњавање и доказивање рачунарског кривичног дела;
Стандарди и супротстављање злоупотреби ИТ.

Okruženje, svakodnevnica

- **Koje su naše ustaljene aktivnosti?**
- **Šta bi moglo da ih ugrozi? (pretnje)**
- **Koliko smo ranjivi?**
- **Kako ćemo se boriti protiv rizika?**

- Umreženi smo!
- Umreženi smo stalno!
- Komuniciramo onlajn
- Informišemo se onlajn (mediji, dešavanja)
- Plaćamo onlajn
- Gledamo TV onlajn
- Booking, Aliexpress…
- Imamo aplikacije za skoro sve aktivnosti koje obavljamo (Kalendar, Endomondno, merač koraka, šta kuvati danas… TV app)

iPhone režim za bezbednu vožnju

https://pcpress.rs/iphone-rezim-za-bezbednu-voznju-i-pristojno-blokiranje-poruka/

- Koliko uređaja imamo?
- Koliko sati dnevno ih koristimo?
- Koliko ključnih informacija je na njima?

Koliko su **ranjivi?**

Kada su ranjivi?

Kako to da sprečimo?

Osnovni pojmovi

Informacije se mogu posmatrati kao nešto što se prenosi nizom simbola

- Alfabetski (karakteri, slova, interpunkcija)
- Fizičke i logičke prirode (knjige ili informacija na računaru)
- Mogu biti merljive - Claude Shannon-ova definicija Teorija informacija

Dodatni aspekti podrazumevaju da je informacija:

- Tačna,
- Blagovremena,
- Kontekstualna i relevantna,
- Svrsishodna,
- Ima vrednost.

Možemo povećati stepen razumevanja određene problematike, smanjiti nesigurnost i uticati na odluke i ishode ponašanja

Sigurnost?

stanje bez opasnosti ili pretnji

Može se primeniti za fizička i logička okruženja.

- Zidovi i brave – Firewall i lozinke
- Može uključivati ljude i procese, kontrole, nadzor, ovlašćenja… (kao na aerodromima).
- **Subjektivni osećaj!**
- Prokativni pristup: Stanje uma!

Informaciona sigurnost

Najopštija definicija koja se može primeniti bez obzira na konkretnu lokaciju informacija je odbrana informacija od neovlašćenog:

- pristupa,
- korišćenja,
- otkrivanja,
- modifikacije,
- nadzora,
- snimanja ili
- uništenja.

Cyber security

Termin **Cyber** Villiam Gibson 1984. u knjizi, "Neuromancer" te iako ga je kasnije kritikovao "suštinski besmislenim" termin je zaživeo i još uvek je u upotrebi.

- **Cyber space**?
- Trenutno jedan od najkorišćenijih računarskih pojmova
- Opisno se predstavlja kao virtuelno računarsko okruženje.
- Nacionalni institut za standarde i tehnologiju (NIST): **CSpace** je globalni domen u okviru informacionog okruženja koji se sastoji od međuzavisne mreže informacionih sistema uključujući i internet, telekomunikacione mreže, računarske sisteme, i ugrađenih procesora i kontrolera.

- **Cyber security**

Association for Computing Machinery (**ACM**)

definiše kao kompjuterski zasnovanu disciplinu koja uključuje:

- tehnologiju,
- ljude,
- informacije i procese kako bi se omogućilo sigurno poslovanje organizacije.

Podrazumeva:

- kreiranje,
- operacije,
- analizu i
- testiranje bezbednosti računarskih sistema.

Cyber security Vs. Informaciona sigurnost

Sigurnost Vs. Bezbednost

Digitalna sigurnost/bezbednost

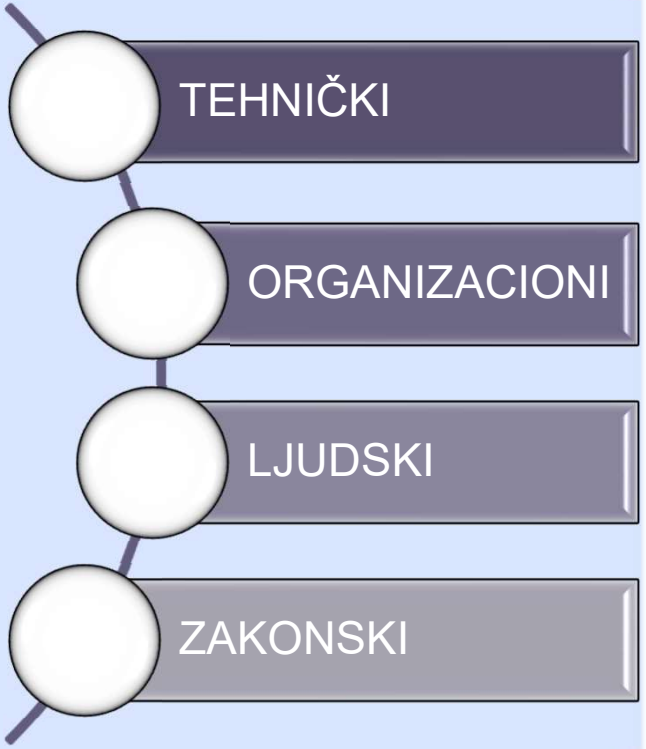
Nas interesuje praktična strana

- U zvaničnim dokumentima Republike Srbije koristi se termin „informaciona bezbednost“ dok je „sajber bezbednost“ prisutnija u međunarodnim dokumentima.
- Međutim, veoma mali broj izvora pravi razliku između pojmova sajber bezbednosti i informacije bezbednost ili njihovog međusobnog odnosa.

NIST definiše:

- **Sajber bezbednost** kao – Sposobnost da se zaštiti sajber prostor od sajber napada.
- **Informacionu bezbednost** kao zaštitu informacija i informacionih sistema od neovlašćenog pristupa, korišćenja, otkrivanja, remećenja, modifikacije ili uništenja kako bi se obezbedili poverljivost, integritet i dostupnost.

- **Interdisciplinarnost**
- pored obaveznog poznavanja tehnologije uključuje i:
- Zakonske regulative;
- Politike bezbednosti;
- Ljudskog faktora;
- Etike;
- Menadžmenta rizika.



Na međunarodnom nivou neizostavno uključuje i politiku, ekonomiju, diplomatiju, psihologiju…

Oblasti koje je neophodno znati:

1. **Sajber odbrana**, bezbednost informacija, kriptografija, bezbednost računara i mreža.
2. **Sajber aktivnosti – dejstva**, sajber napadi, pen test, obrnuti inženjering, kriptoanaliza.
3. **Digitalna forenzika**, hardverska i softverska forenzika, mobilnih uređaja, sajber kriminal i zakonska regulativa.
4. **Sajber fizički sistemi**, sistemi za nadzor i kontrolu podataka (SCADA), internet stvari (IOT), industrijski kontrolni sistemi.
5. **Razvoj bezbednog softvera**, dizajn sigurnog sistema, sigurno kodiranje, primenu, održivost i upotrebljivost.

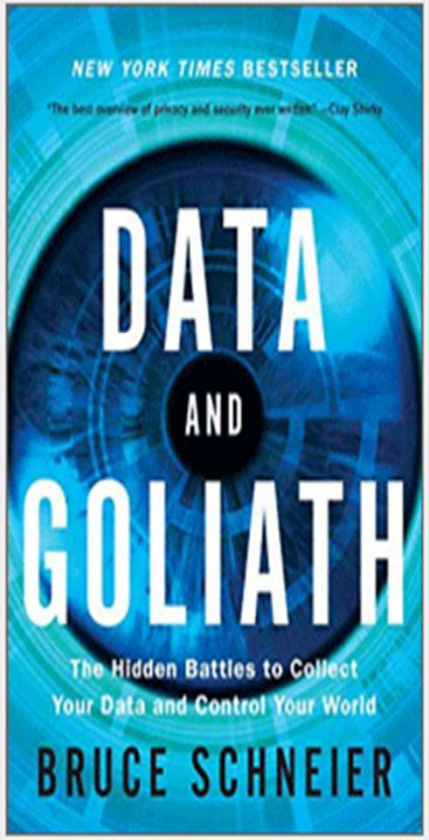
6. **Bezbednosna politika i zakonska regulativa,** postoji niz propisa koji se primenjuju na sajber sisteme i operacije, i naravno sajber zakone kao što su zaštita podataka, intelektualne svojine zloupotreba računara itd. Neophodan tehnički aspekt da bi se bolje razumela regulativa.

7. **Upravljanje sajber rizikom,** oporavak od katastrofe, mere kontinuiteta poslovanja, evaluacija sigurnosti (npr. pitanja usklađenosti).

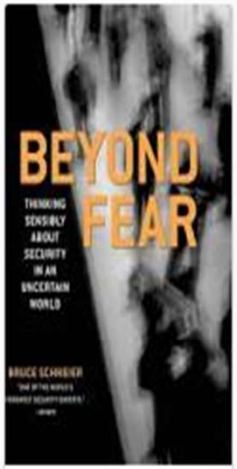
8. **Ljudsko ponašanje,** vezano za sajber sisteme i operacije, kao što su socijalni inženjering, korišćenje društvenih mreža, korisničko iskustvo i organizaciono ponašanje.

"Samo amateri napadaju mašine, profesionalci ciljaju ljude" čuvena je rečenica Bruce Schneier, američkog kriptografa, stručnjaka za IT bezbednost. (https://www.schneier.com/)

Bruce Schneier

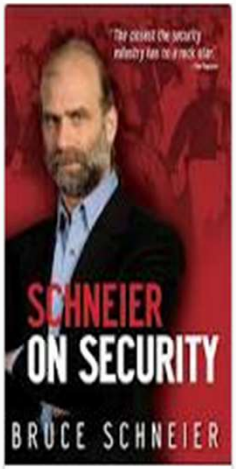


March 2015
W. W. Norton & Company
320 Pages

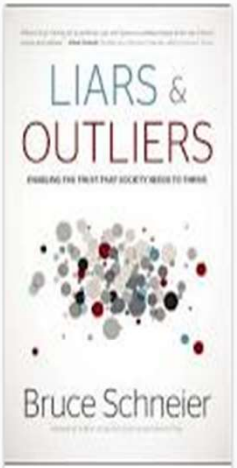


Beyond Fear: Thinking Se...
2003.

Secrets and Lies: Digital ...
2000.



Schneier on Security
2008.



Liars and Outliers
2012.

Practical Cryptography
2003.

Cryptography Engineering:...
2010.

Data and Goliath

The Hidden Battles to Collect Your Data and Control Your World

A Book by Bruce Schneier

A New York Times Best Seller

om/talks/bruce_schneier

10 Steps To Cyber Security

Defining and communicating your Board's Information Risk Management Regime is central to your organisation's overall cyber strategy. CESG recommend you review this regime - together with the nine associated security areas described below - in order to protect your business against the majority of cyber threats.

Network Security

Protect your networks against external and internal attack. Manage the network perimeter. Filter out unauthorised access and malicious content. Monitor and test security controls.

Malware Prevention

Produce relevant policy and establish anti-malware defences that are applicable and relevant to all business areas. Scan for malware across the organisation.

Monitoring

Establish a monitoring strategy and develop supporting policies. Continuously monitor all ICT systems and networks. Analyse logs for unusual activity that could indicate an attack.

Incident Management

Establish an incident response and disaster recovery capability. Produce and test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to law enforcement.

User Education and Awareness

Produce user security policies covering acceptable and secure use of the organisation's systems. Establish a staff training programme. Maintain user awareness of the cyber risks.

Home and Mobile Working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline build to all devices. Protect data both in transit and at rest.

Secure Configuration

Apply security patches and ensure that the secure configuration of all ICT systems is maintained. Create a system inventory and define a baseline build for all ICT devices.

Removable Media Controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing into the corporate system

Managing User Privileges

Establish account management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

SAD procenile da su sajber napadi veća pretnja od terorizma!

26.02 19:19 | Digital

Teroristički napadi na Pariz

Postoje informacije da su korišćene Sony PS4 konzole za:

- Slanje poruka
- Glasovnu komunikaciju
- Komunikaciju tokom igre


REALNOST?

If you've used your cell phone today — or any other wireless device that uses Bluetooth technology — someone could be watching you.

John Hering, a student at the University of Southern California, has developed the BlueSniper rifle, a tool that looks like a big gun which can "attack" a wireless device from more than a mile away — several times the 328-foot maximum range of Bluetooth.

Hering, cofounder of a wireless security think tank called Flexilis, says he uses the "rifle" only to determine security vulnerabilities, not to actually hack wireless devices to obtain personal information.

"Whenever we're working on these tests, we never access anyone's data," he tells Michele Norris. "We're simply assessing the vulnerabilities and what's possible."

Hering says his goal is to boost awareness of the vulnerabilities in Bluetooth. But in laboratory testing, Hering says, his company has been able to access SMS messages, passwords, phonebook contacts and camera phone photos from Bluetooth-enabled phones.

John Hering and his BlueSniper rifle, which he says can sniff out and hack Bluetooth-enabled wireless devices more than a mile away.

Humphrey Cheung/TomsNetworking.com

TECHNOLOGY

'Rifle' Sniffs Out Vulnerability in Bluetooth Devices

Updated April 13, 2005 · 4:05 PM ET

Published April 13, 2005 · 12:00 AM ET

Listen

All Things Considered

+ Playlist Download Embed

If you've used your cell phone today — or any other wireless device that uses Bluetooth technology — someone could be watching you.

John Hering, a student at the University of Southern

SHARE

2015 Cybersecurity Predictions

Lookout

- **There will no longer be a technology industry. All industries will be technology industries.**
- **Cybercrime will just be called crime!**
- **Companies will replace reactive security with predictive security**
- **Pre-installed malware will increase**
- **Vulnerable apps will become a bigger problem than vulnerable operating systems**
- **United States will become more of a target for mobile malware**

https://www.lookout.com/resources/reports/predictions


SURFACE WEB
Google
Bing
Wikipedia
DEEP WEB
Academic Information
Medical Records
Legal Documents
Scientific Reports
Subscription Information
Contains 90% of the information on the Internet, but is not accessible by Surface Web crawlers.
Social Media
Multilingual Databases
Financial Records
Government Resources
Competitor Websites
Organization-specific Repositories
(DARK WEB)
A part of the Deep Web accessible only through certain browsers such as Tor designed to ensure anonymity. Deep Web Technologies has zero involvement with the Dark Web.
Illegal Information
TOR-Encrypted sites
Political Protests
Drug Trafficking sites
Private Communications


Web vi
Web un peu
mais toujou
moteurs de
4chan
x550
TorProject.org
anonymous marketplace
.Onion
The Hidden Wiki
Web i

REALNOST?

Šta beše sigurnost?

- Kada se govori o sigurnosti uopšte, a posebno o sigurnosti u sajber okruženju važno je naglasiti da se sigurnost ne sme doživeti kao gotov proizvod ili konačno stanje.
- **Sigurnost je proces održavanja nivoa prihvatljivog rizika!**

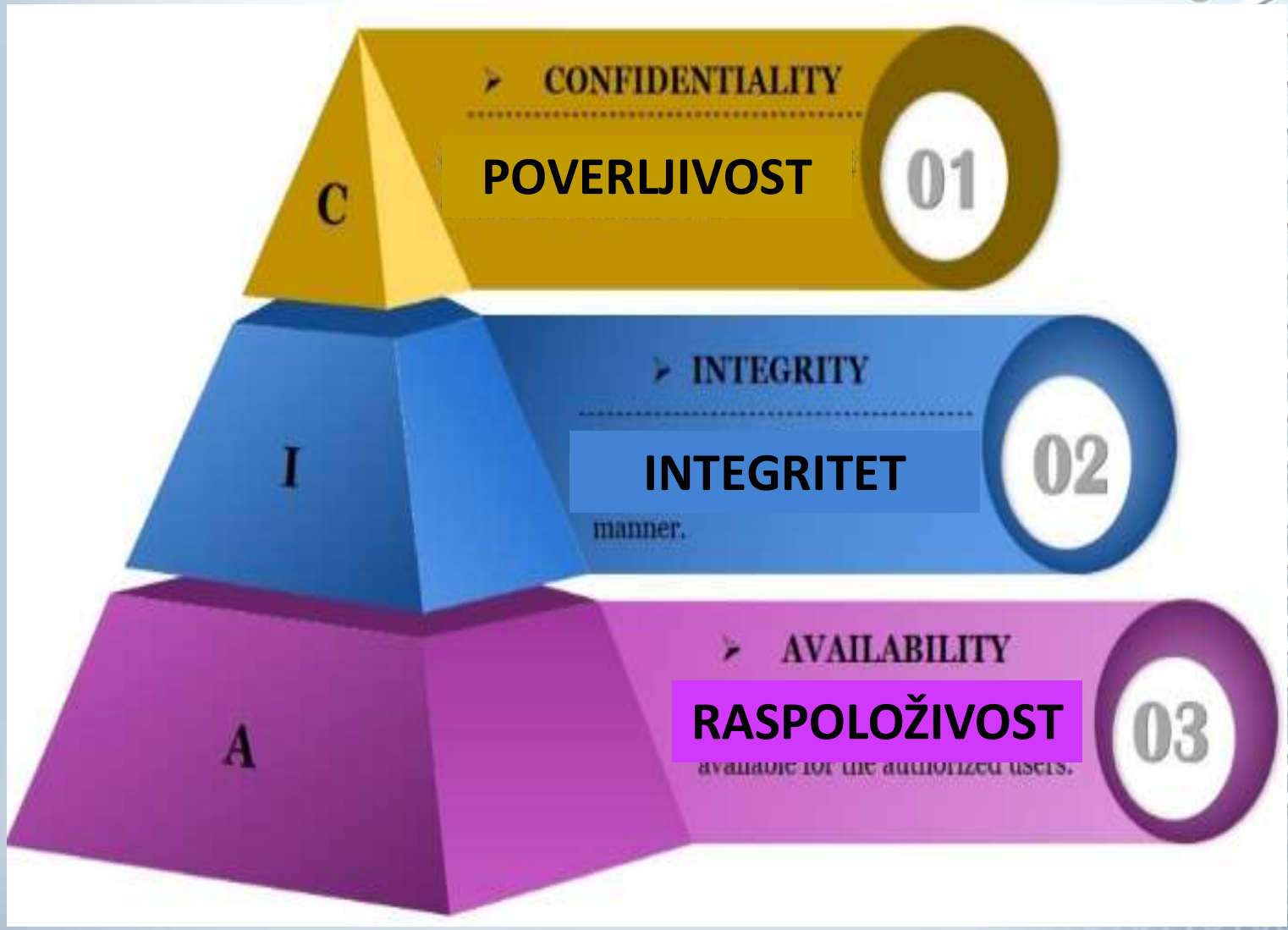
Proces ≠ gotov proizvod

- **Sigurnost se ne može kupiti kao proizvod ili usluga**
- **To je proces u kome se koriste:**
  - Različiti proizvodi i usluge
  - Procedure i pravila

  U kome se sprovodi:
  - Konstanta edukacija
  - Podizanje nivoa svesti
  - Stalno praćenje dešavanja u ovoj oblasti (koliko često?)

[1] D. Pleskonjić, N. Maček, B. Đorđević, M. Carić „Sigurnost računarskih sistema i mreža“

Osnovni koncept sigurnosti
CIA trijada



Poverljivost (Confidentiality).

- ekvivalent privatnosti.
- zaštita podataka od neovlašćenog pristupa i
- primena mera kako bi se osiguralo da samo ovlašćena lica mogu pristupiti informacijama.

Integritet (Integrity).

- Zaštita menjanja podataka od strane neovlašćenih lica ili procesa.
- Integritet se održava kada podaci ostaju nepromenjeni tokom skladištenja, prenosa, i upotrebe

Raspoloživost (Availability).

- Pravovremeno pristupanje podacima od strane ovlašćenih lica. Raspoloživost je moguća kada sve komponente informacionog sistema rade pravilno.

- **Koja je komponenta najvažnija**?

  (sve tri su podjednako važne)

- **Da li mogu postojati specijalne situacije kada neka od komponenti ima blagi prioritet?**

  (- poverljivost može biti važnija kada se radi o vlasničkim podacima kompanije ili podacima koji se odnose na lične podatke.

  - Integritet je prioritet kod finansijskih informacija, primer banaka.

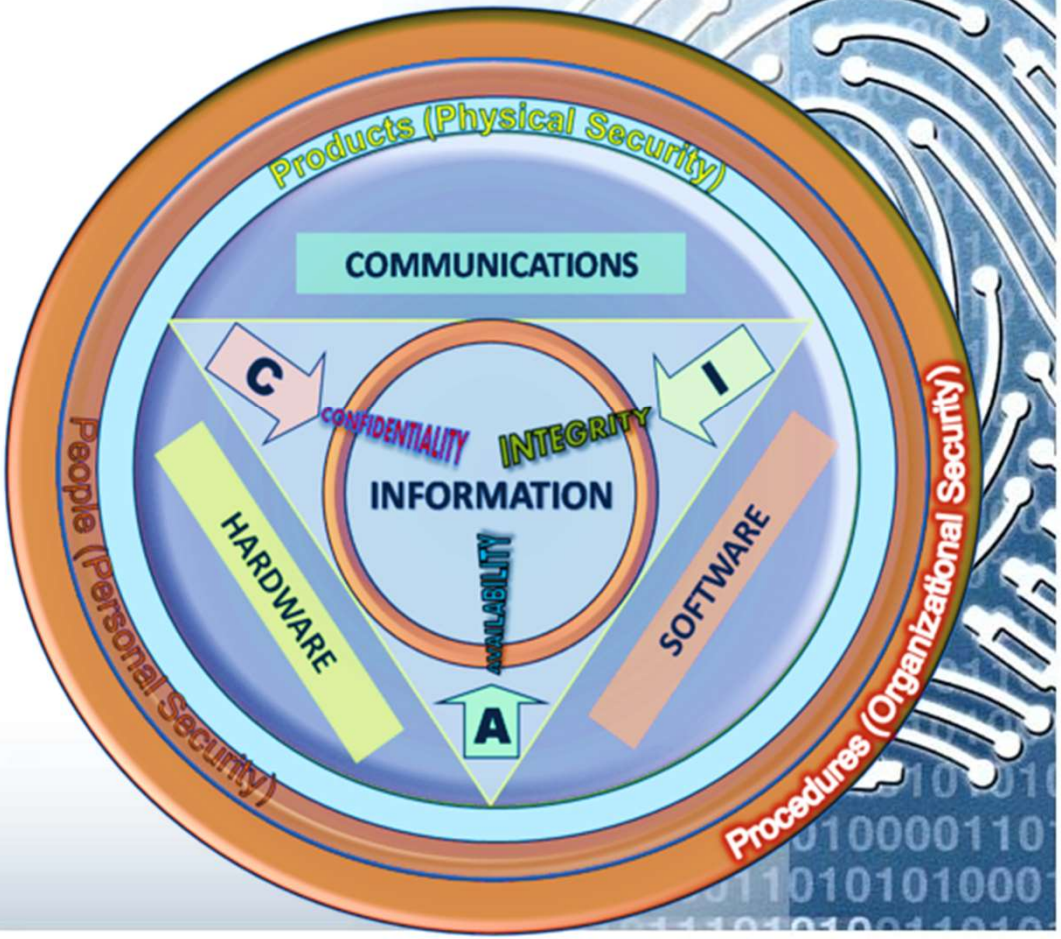
  - Raspoloživost je u prvom planu kod važnih saopštenja za javnost npr. sajt vlade).

Zbog čega su nam bitni sigurnost i zaštita IS?

Šta zapravo štitimo?

CIA trijada obuhvata:

- **Hardver (računare, servere, pametne telefone itd.),**
- **Softver (operativni sistemi, kao i aplikacije) i**
- **Komunikacione tehnologije (prekidači, ruteri, Wi-Fi pristupne tačke, bazne stanice, itd.).**
- **Ove osnovne komponente su u kontekstu sistema, ljudi i procesa**



Sigurnosne usluge (namena)

- **Poverljivost, privatnost** – Poverljivost je omogućavanje pristupa podacima samo ovlašćenim korisnicima a privatnost dostupnost informacija samo korisnicima kojima je namenjenia i nikom više.
- **Provera idenditeta** – omogućavanje pristupa tek nakon logovanja (korisničko ime, lozinka) što obezbeđuje uvid u ponašanje korisnika i lakšu detekciju prilikom spornih situacija.
- **Integritet** – usluga obezbeđivanja celovitosti podataka.Zaštita od neovlašćenog, nepredviđenog ili nenamernog modifikovanja.
- **Neporicanje** – usluga koja obezbeđuje da korisnik koji je poslao ili promenio poruku ne može naknadno tvrditi da to nije uradio.
- **Kontrola pristupa** – omogućava samo objektu sa proverenim identitetom i odgovarajućim ovlašćenjima upotrebu usluga sistema. To znači da određuje koi ma pravo da pristupi resursima i na koji način.

Osnovni principi sigurnosti:

- Sigurnost je proces koji se zasniva na četiri osnovna koraka
  - Procena,
  - Zaštita,
  - Otkrivanje,
  - Odgovor.
- **Ne postoji apsolutna sigurnost** !

  Veće ulaganje u sigurnost samo **smanjuje, ne otklanja u potpunosti** izloženost sistema riziku

  Sigurnosni mehanizmi i procedure smanjuju udobnost rada ili pogoršavaju performanse sistema
- Uz sve primenjene metode zaštite nikako **ne smemo zanemariti ljudski faktor**

Pojam i ciljevi zaštite

Pod pojmom zaštite se podrazumevaju :

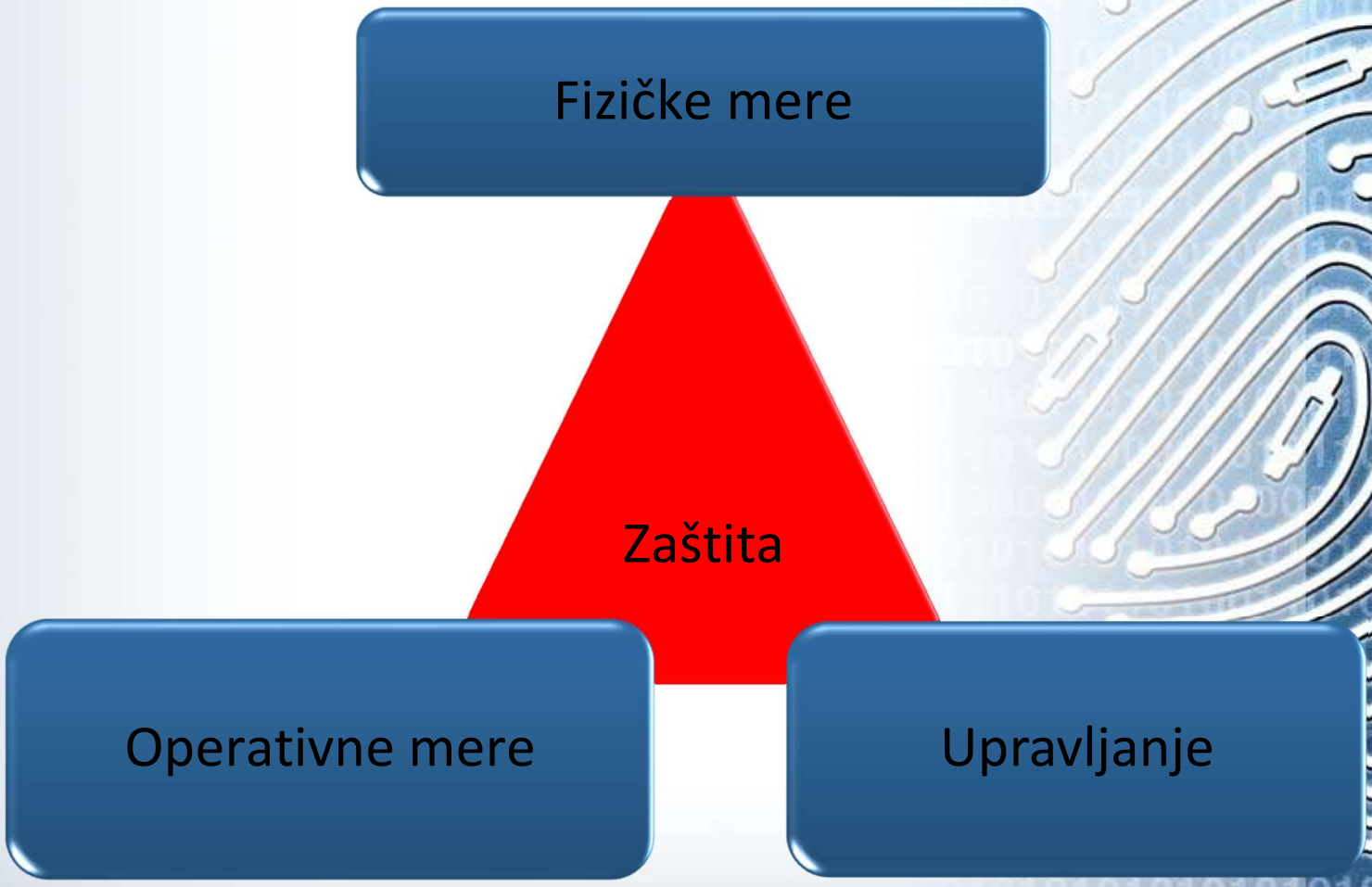
- **sredstva,**
- **mere i**
- **aktivnosti**

namenjeni za sprečavanje ili umanjenje ugrožavanja materijalnih dobara, prava i života ljudi, životne sredine, države i društva.

U domenu IT pojam zaštite obuhvata

- **zaštitu IKT opreme,**
- **infrastrukture,**
- **programa i podataka.**

Trougao zaštite



Fizičke mere

- Sprečavanje fizičkog pristupa neovlašćenih lica opremi i podacima.
- Fizička zaštita se postiže relativno jednostavno.

I FM: smanjenje privlačnosti fizičke lokacije.

II FM: detekcija upada ili kradljivca.

Korisnik mora znati gde je došlo do provale, šta nedostaje i kako je došlo do gubitaka.

III FM: oporavak firme nakon krađe ili gubitka ključnih podataka i sistema.

Oporavak zahteva detaljno planiranje, razmišljanje i testiranje.

Vežba 1.1: Analiza fizičkog okruženja

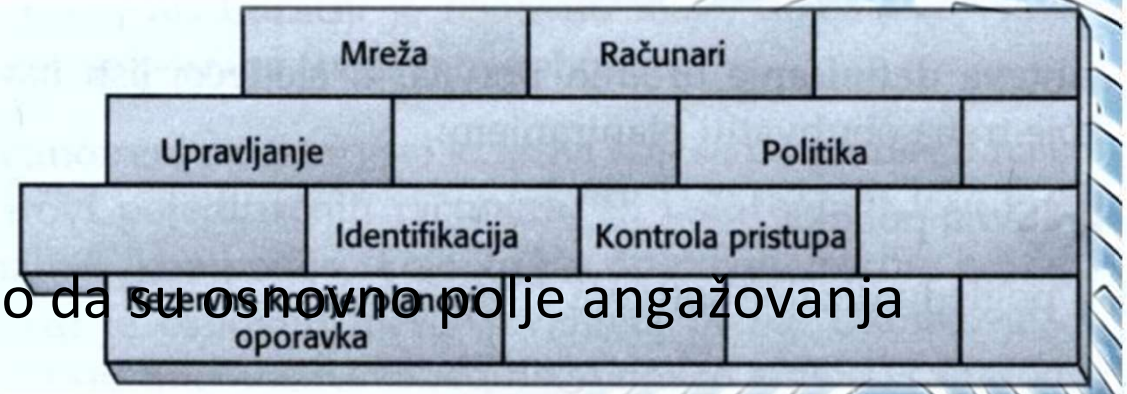
Kao administrator sistema zaštite, morate postaviti sebe u ulogu "uljeza", odnosno osobe koja želi da prodre u Vaš poslovni prostor. Zamislite da ste lice izvan organizacije koje želi da pristupi njenom serveru i da ga ošteti. Nemojte razmišljati o tome kako ćete ukrasti podatke sa servera, već samo o tome kako ćete u njega naliti vode. Pokušajte da odgovorite na sledeća pitanja:

1. Kako ćete ući u zgradu? Da li su za to potrebni ključ ili neki kod? Da li postoji neka zaštita ulaza - čuvar, recepcionar ili kamera?
2. Kako ćete doći do sprata na kome se nalazi server? Da li su liftovi zaključani ili ih može koristiti svako?
3. Kako ćete pronaći server? Da li se on nalazi u nekoj kancelariji ili u zasebnoj prostoriji? Ukoliko je u zasebnoj prostoriji, da li su vrata te prostorije obezbeđena?
4. Kada dođete do servera, da li će neko primetiti šta radite? Da li se u prostoriji sa serverom nalaze stakleni prozori? Da li se server može videti sa daljine? Da li će neko pitati šta radite tu?

Ako možete jednostavno da odgovorite na sva navedena pitanja, pri čemu i u sistemu zaštite postoje propusti, postoji velika opasnost da neko može nauditi poslovanju Vaše firme. Konačno, pokušajte da odgovorite na slična pitanja, ali se nemojte stavljati u ulogu nekoga izvan organizacije, već u ulogu službenika iz računovodstva koji nije dobio željeno unapređenje i sada želi da se osveti firmi.

Operativne mere zaštite

- Način obavljanja poslovnih funkcija u organizaciji.
- Obuhvataju:
  - Računare,
  - Mreže,
  - Komunikacione sisteme i
  - Rad sa dokumentima.
- Pokrivaju široku oblast tako da su osnovno polje angažovanja profesionalnog osoblja.
- Uključuju:
  - Kontrolu pristupa,
  - Identifikaciju i
  - Topologiju zaštite nakon instaliranja mreže.



To znači sve što nije u direktnoj vezi sa dizajnom ili fizičkom zaštitom mreže.

Vežba 1.2: Analiza operativnog okruženja

U ovoj vežbi ćemo izvršiti analizu operativnog okruženja u Vašoj firmi, u potrazi za načinom na koji neka "spoljašnja" osoba može prodreti do Vaših podataka. Nemojte razmišljati o merama zaštite koje već postoje, već se skoncentrišite na mogućnosti da nepoznata osoba pristupi Vašoj mreži. Pokušajte da odgovorite na sledeća pitanja:

1. Kako korisnici pristupaju Internetu? Da li bilo ko od njih koristi pristup pomoću komutirane (dial-up) linije? Da li koristite privatne ili javne IP adrese?
2. Da li u mreži postoje bežične pristupne tačke? Da li mobilni korisnik sa prenosnim računarom može podesiti svoj sistem da bi se uključio na mrežu?
3. Da li postoje ulazne linije biranja? Može li korisnik ući na mrežu pozivom od kuće?
4. Da li koristite Terminal Services? Da li se kompletne sesije na serveru odvijaju kao udaljene?

Osiguranje mreže obuhvata znatno širu oblast od proste zaštite onoga što je smešteno između zidova Vaše kancelarije. Potražite prolaze kroz koje "uljezi" mogu dopreti do Vaše mreže, a da uopšte ne prođu kroz ulazna vrata u zgradu.

Upravljanje

- Osnovna uputstva pravila i procedure za implementaciju zaštićenog okruženja.
- Neke od oblasti koje treba obuhvatiti planiranjem:
  - Administrativna politika,
  - Zahtevi u pogledu dizajna softvera,
  - Planovi oporavka sistema nakon težih padova,
  - Oblast zaštite podataka,
  - Politika zaštite,
  - Pravila upotrebe,
  - Pravila koja definišu upravljanje korisnicima.

Vežba 1.3: Definisanje i provera procedura

Iznenađujući je broj firmi koje tvrde da poseduju definisana poslovna pravila, ali ih ne mogu pronaći kada se za to ukaže potreba. Pokušajte da odgovorite na sledeća pitanja:

1. Da li Vaša kompanija raspolaže jasno definisanom administrativnom politikom - koja pravila su definisana u njoj i gde se ona može naći?
2. Kada su zahtevi u pogledu dizajna softvera poslednji put proveravani i ažurirani? Da li se ti zahtevi uvek predočavaju isporučiocima?
3. Kada je poslednji put proveren plan za oporavak računarskog sistema nakon težih padova? Da li svi administratori poznaju taj plan?
4. Da li su pravila za zaštitu podataka lako dostupna?
5. Koliko često se vrši ažuriranje politike zaštite? Da li se ona ažurira pri svakoj izmeni softvera?
6. Da li se pravila za upotrebu nalaze u priručnicima koji su podeljeni zaposlenima? Da li zaposleni moraju da potpišu izjavu da poznaju ta pravila? Da li izmene pravila dopiru do korisnika i na koji način oni potvrđuju da su im poznate izmene i da ih razumeju?
7. Postoji li dokumenat u kome su jasno definisana pravila u vezi sa korisnicima? Da li se ta pravila mogu primeniti i kada je administrator odsutan (na sastanku)?

!!!

Osnovni preduslov za primenu zaštite je da rukovodstvo razume problem:

- **opasnosti koje mogu ugroziti informacioni sistem,**
- **uslove i ambijent koji pogoduju nastajanju neželjenih pojava, kao i**
- **moguće negativne (štetne) posledice koje zbog toga mogu nastupiti.**

Potencijalni izazivači ugrožavanja IS mogu biti svrstani u sledeće kategorije

"Viša sila"	Hardversko-softverski nedostaci	Ljudski faktor
▪ Zemljotres ▪ Oluja ▪ Poplava ▪ Požar ▪ Visoka temperatura ▪ Nestabilnost napajanja ▪ Elektromagnetna zračenja ▪ Vanredne prilike ▪ Ratno stanje	• Kvarovi na informatičkim uređajima • Tehnička greška infra-strukture • Greške u kontrolnim ili upravljačkim programima • Greške u aplikativnim programima	• sa atributom nenamernosti Nehat Nestručnost Nedisciplina Loša organizacija Zamor • sa atributom namernosti Narušavanje privatnosti Odavanje tajne Pronevere Sabotaže Falsifikovanje Stvaranje i distribucija virusa Elektronsko uznemiravanje Krađa računarskih usluga

Ciljevi zaštite

Prevencija

sprečavanje ugrožavanja

Detekcija

otkrivanje ugrožavanja

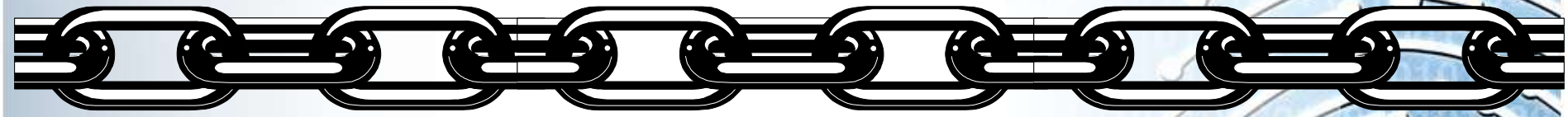
Odgovor

dejstvovanje u slučaju nastanka ugrožavanja i otklanjanje posledica

Da bi se ispunili postavljeni ciljevi, zaštita mora biti planirana, projektovana i realizovana sveobuhvatno, organizovano, stručno i racionalno.

Zaštita je onoliko jaka koliko je jaka najslabija karika u njoj!

Lanac bezbednosti



Karike u lancu

(Netehnološki orjentisane)

- ✓ Fizička bezbednost
- ✓ Personalna bezbednost
- ✓ Proceduralna bezbednost
- ✓ Upravljanje rizikom
- ✓ Politika bezbednosti
- ✓ Planiranje bezbednosti
- ✓ Upravljanje vanrednim događajima

Karike u lancu

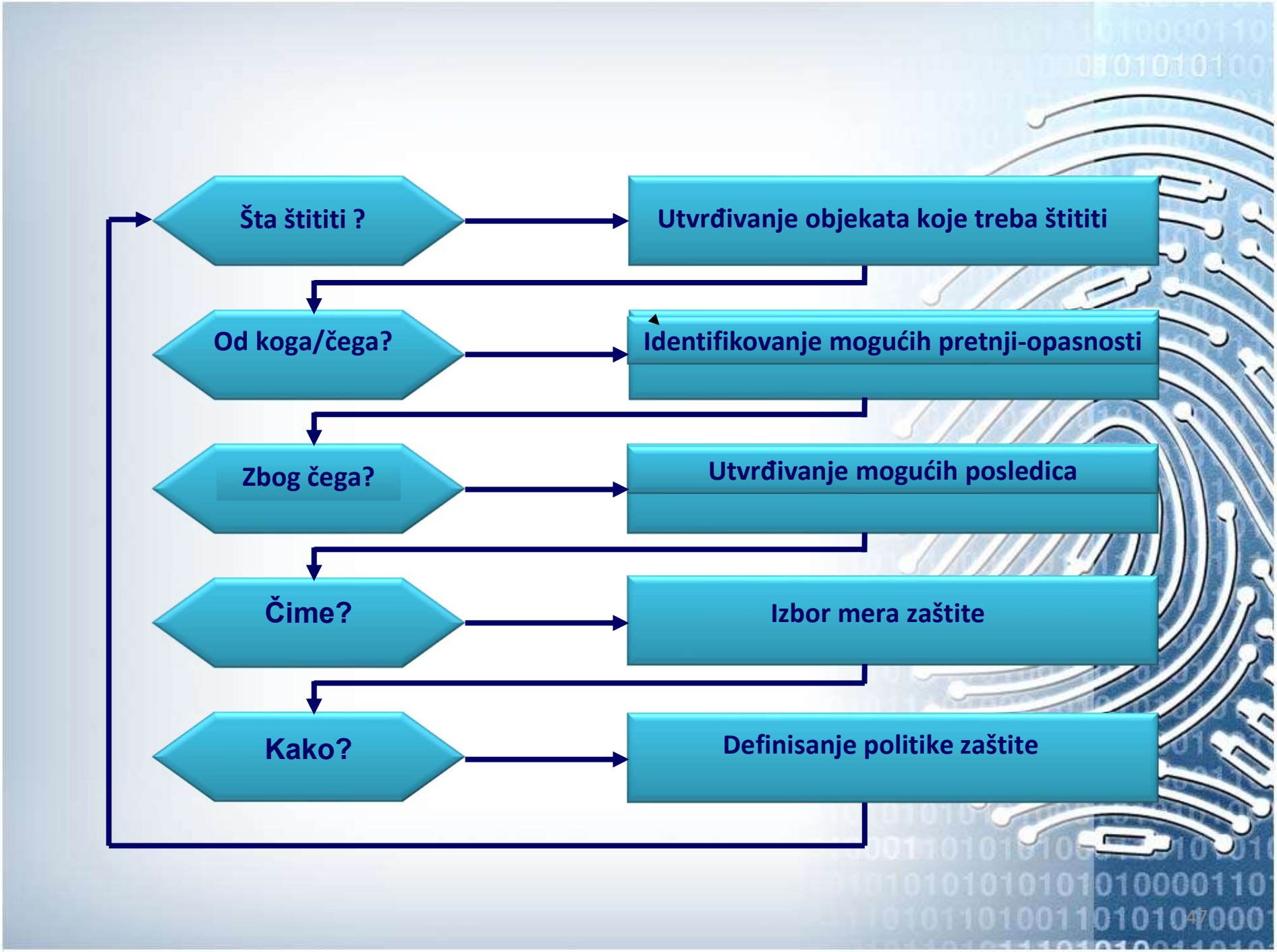
(Tehnološki orjentisane)

- ✓ Mehanizmi kontrole pristupa
- ✓ Mehanizmi identifikacije i autentifikacije
- ✓ Mehanizmi evaluacije
- ✓ Mehanizmi šifrovanja
- ✓ Mrežni zaštitni mehanizmi
- ✓ Smart kartice
- ✓ Biometrija

Polazni elementi pri uvođenju zaštite

Polazni elementi pri uvođenju zaštite su odgovori na sledeća pitanja:

- Šta štititi?
- Od koga ili čega štititi?
- Zbog čega štititi?
- Čime štititi? i
- Kako štititi?


Šta štititi ?
Utvrđivanje objekata koje treba štititi
Od koga/čega?
Identifikovanje mogućih pretnji-opasnosti
Zbog čega?
Utvrđivanje mogućih posledica
Čime?
Izbor mera zaštite
Kako?
Definisanje politike zaštite

http://www.interpol.int/

INTERPOL's six priority crime areas

Drugs and criminal organizations
Tackling the growing problem of drug abuse and trafficking, often linked to other crimes.

Financial and High-tech Crime
Combating counterfeiting, payment card fraud, intellectual property and cyber-crime.

Fugitives
Tracing fugitives, who threaten public safety and undermine criminal justice systems.

Public safety and terrorism
Countering terrorism, which threatens public safety and world security.

Trafficking in human beings
Fighting abuse and exploitation of people, which breach human rights and destroy lives.

Corruption
'Working together towards a corruption-free world by promoting and defending integrity, justice and the rule of law.'


CBRNE


Corruption


Crimes against children


Crimes in sport

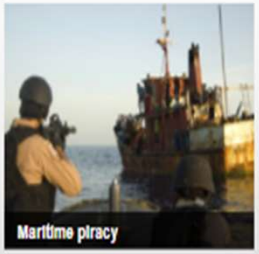

Cybercrime


Drugs


Environmental crime


Financial crime


Firearms trafficking

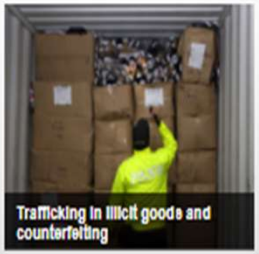

Maritime piracy


Organized crime


Pharmaceutical crime

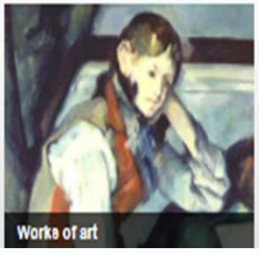

Terrorism


Trafficking in human beings


Trafficking in illicit goods and counterfeiting

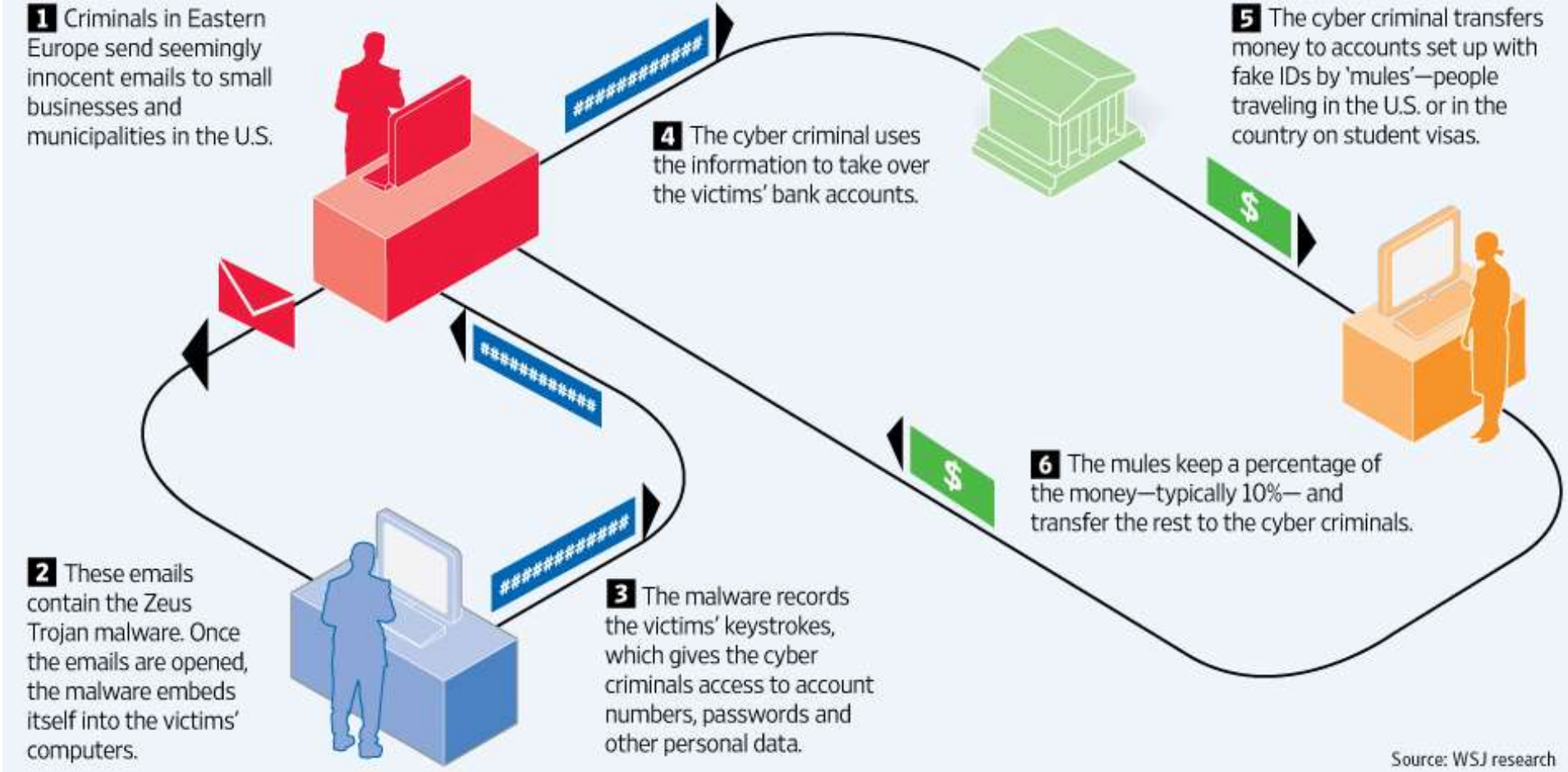
Vehicle crime


War crimes


Works of art

Cyber Banking Fraud

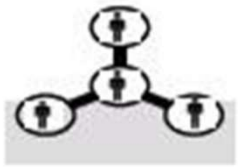
Automated Teller | How cyber criminals allegedly siphoned millions of dollars out of U.S. banks



Source: WSJ research

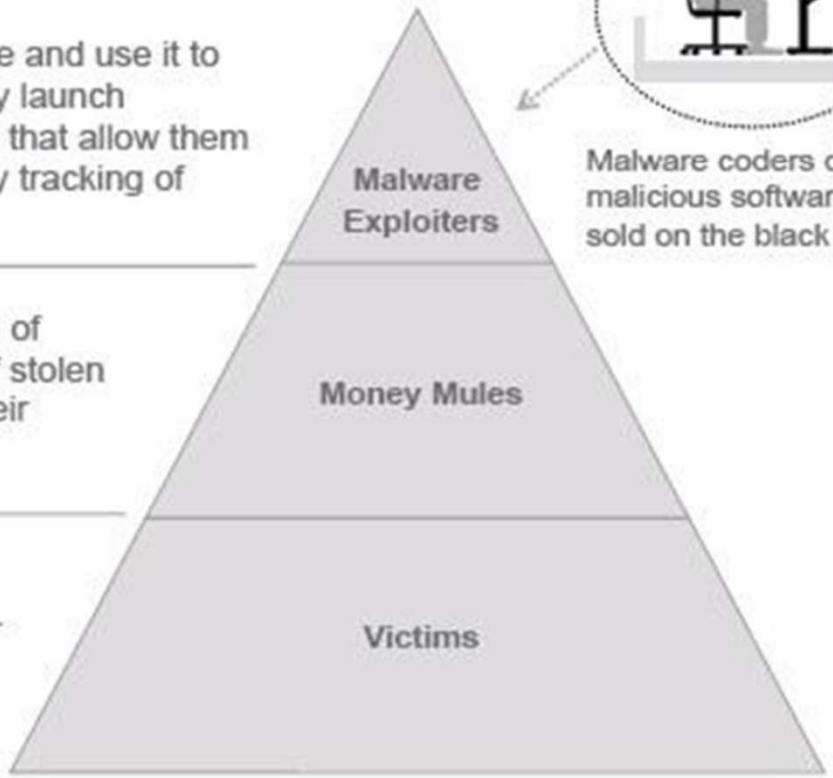
Cyber Theft Ring

Malware exploiters purchase malware and use it to steal victim banking credentials. They launch attacks from compromised machines that allow them to transfer stolen funds and deter any tracking of their activities.



Money mule networks are comprised of individuals engaged in the transfer of stolen funds who retain a percentage for their services.

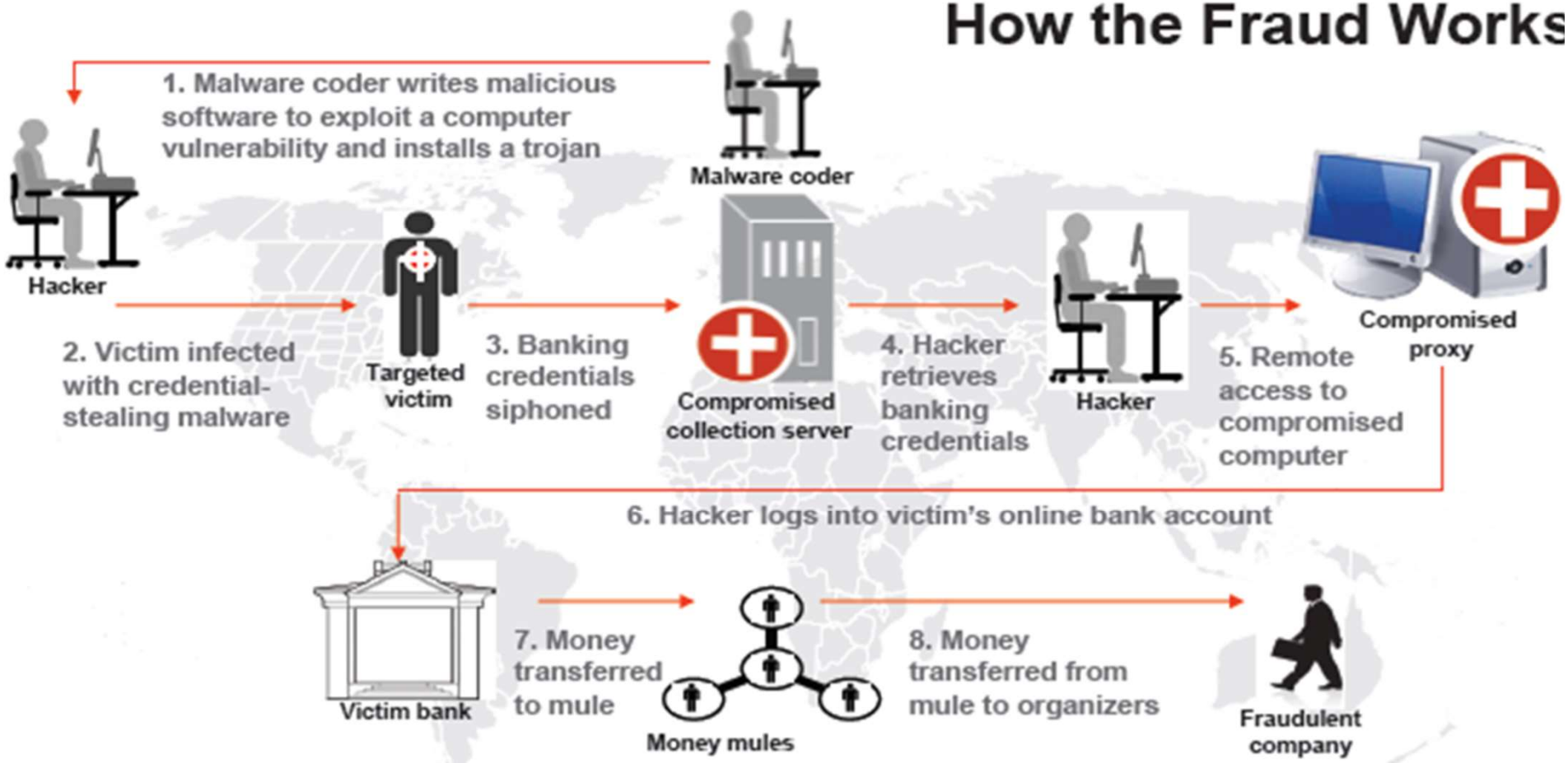
Victims include individuals, businesses, and financial institutions.



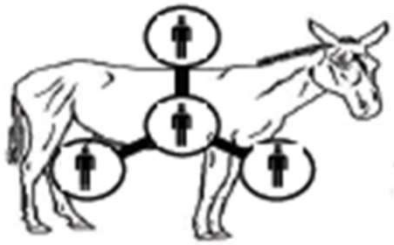
Malware coders develop malicious software that is sold on the black market.

http://www.fbi.gov/news/stories/2010/october/cyber-banking-fraud

How the Fraud Works



Victims are both financial institutions and owners of infected machines.

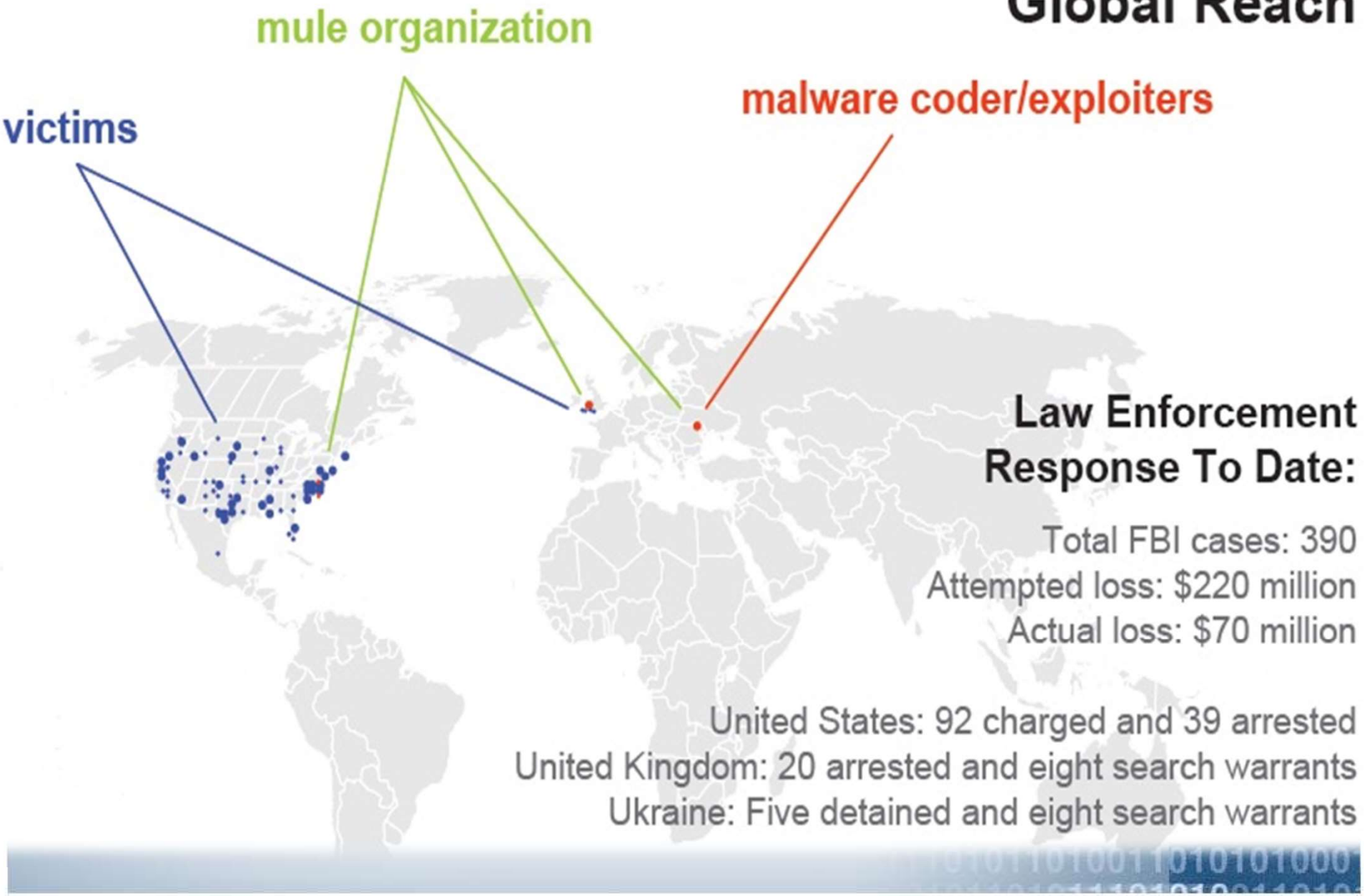


Money mules transfer stolen money for criminals, shaving a small percentage for themselves.

Criminals come in many forms:

- Malware coder
- Malware exploiters
- Mule organization

Global Reach

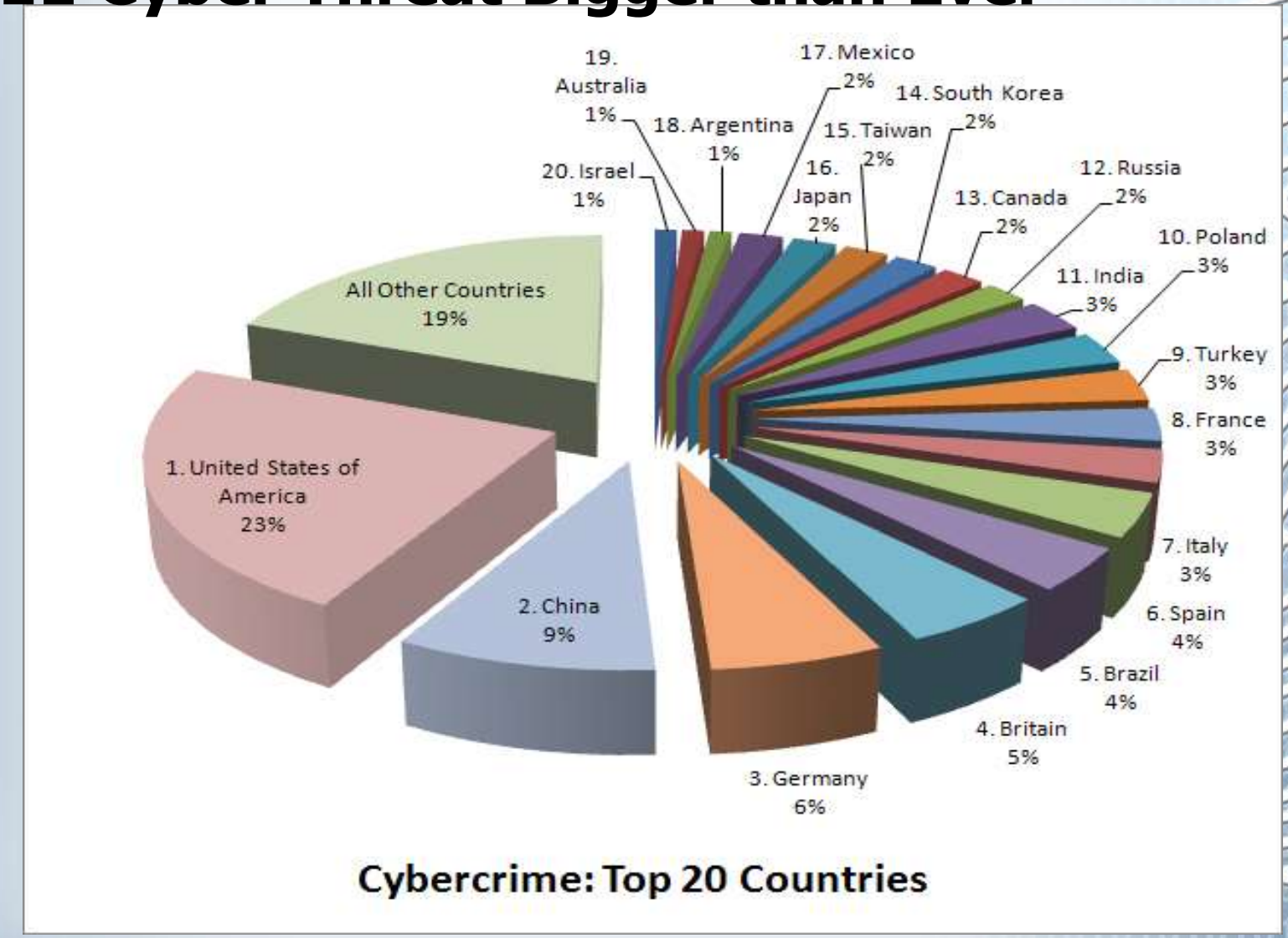


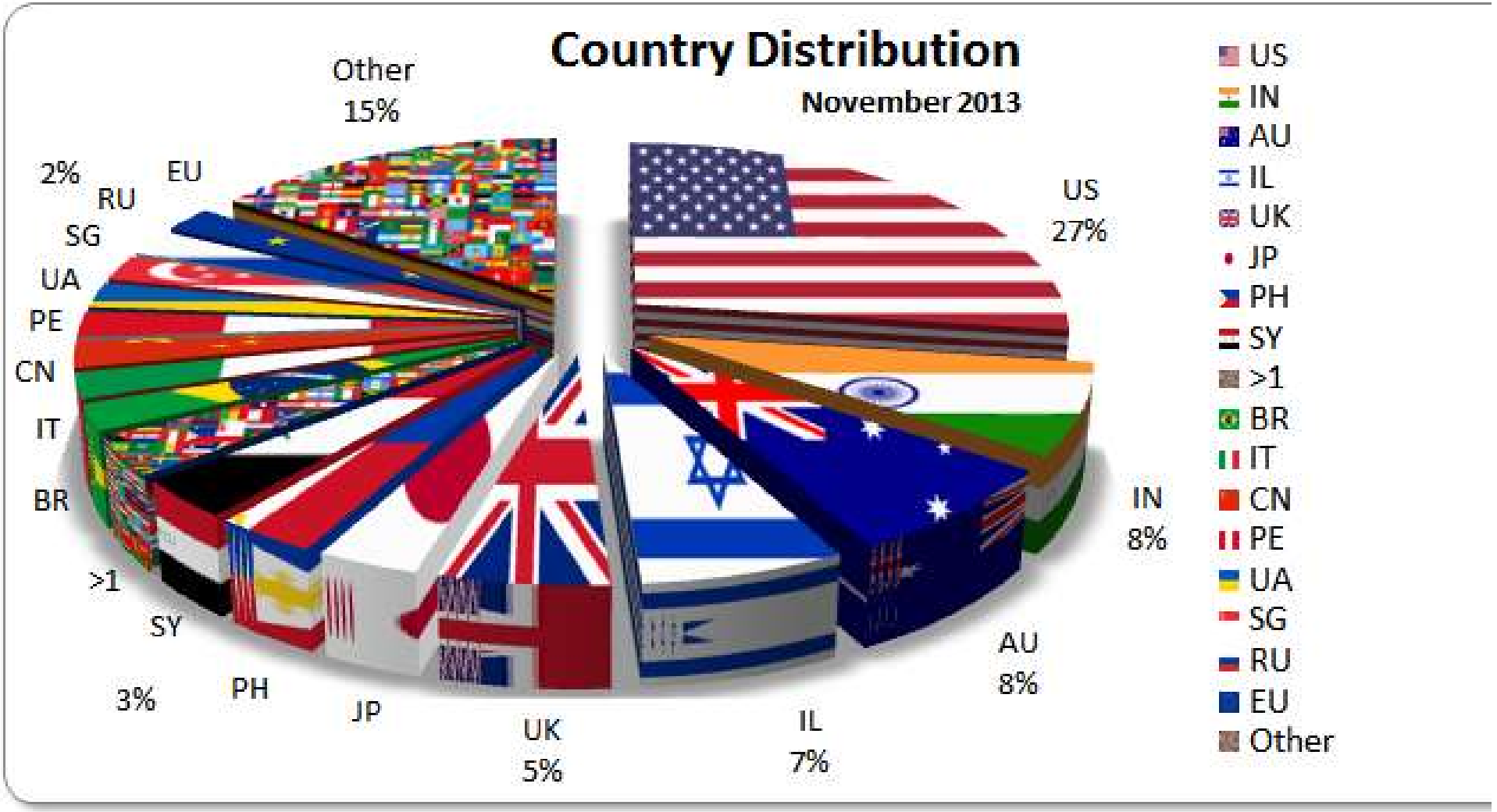
Law Enforcement Response To Date:

Total FBI cases: 390
Attempted loss: $220 million
Actual loss: $70 million

United States: 92 charged and 39 arrested
United Kingdom: 20 arrested and eight search warrants
Ukraine: Five detained and eight search warrants

FBI Warning:
2011 Cyber Threat Bigger than Ever

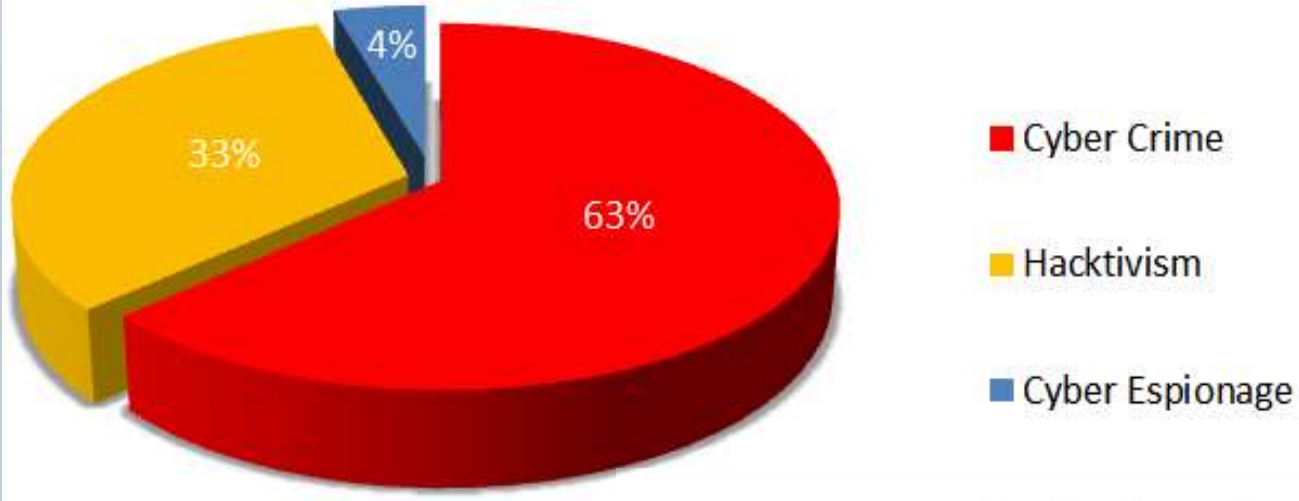




Izvor: http://hackmageddon.com/2013/12/08/november-2013-cyber-attacks-statistics/

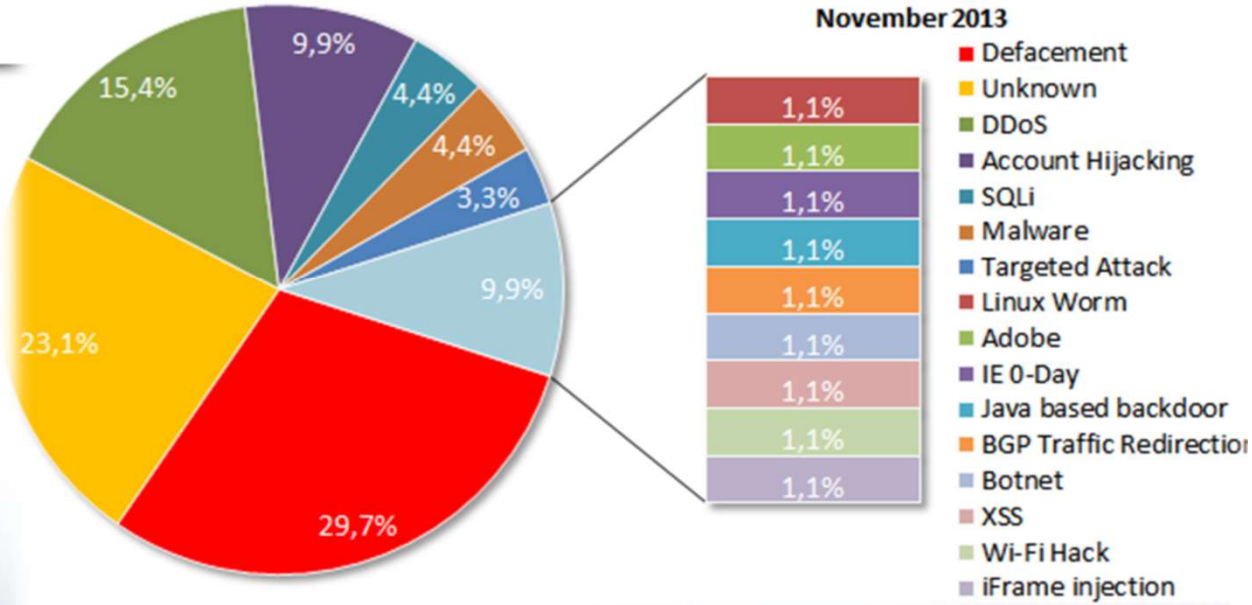
Motivations Behind Attacks

October 2013



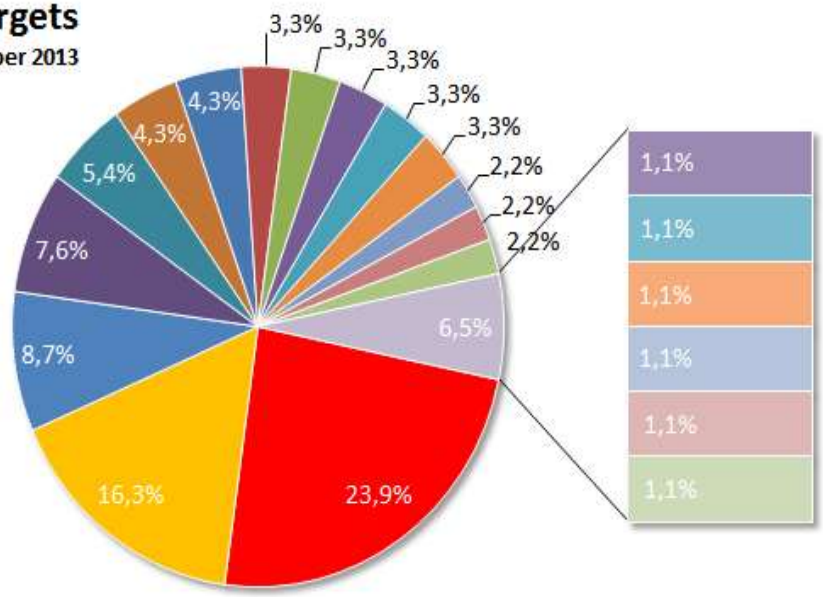
Distribution of Attack Techniques

November 2013



Distribution Of Targets

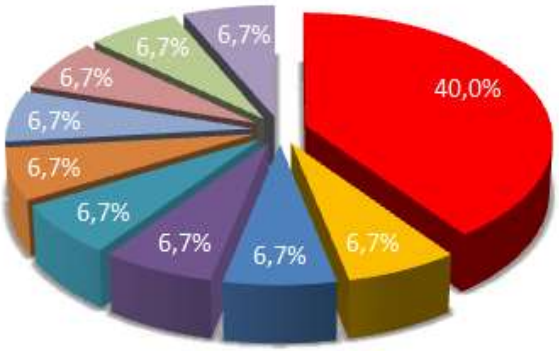
October 2013



- Government
- Industry
- Organization
- Education
- Internet Services
- Law Enforcement
- Telco
- Health
- Finance
- News
- Single Individual
- Online Services
- Military
- Transport
- Social Network
- Web Hosting
- ISP
- Online Forum
- Mobile Operator
- Torrent
- Bitcoin Forum

Industry Fragmentation

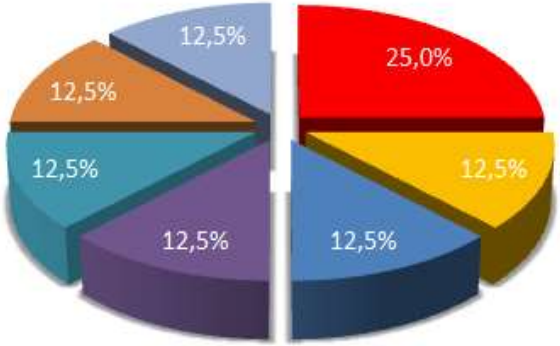
October 2013



- Software
- Pharmaceuticals
- Online Services
- Retail
- Defense
- Order Fulfillment
- Business Information
- Job Search
- Real Estate
- Financial Services

Organization Fragmentation

October 2013



- United Nations
- Religion
- Enterainment
- Gas and Oil
- Sport
- Human Rights
- Political Party

The Top 10 safest locations in terms of the local infection rate are:

Japan	9,10%
Denmark	12,10%
Finland	13,60%
Sweden	14,60%
The Czech Republic	14,80%
Switzerland	15,10%
Ireland	15,20%
The Netherlands	16,20%
New Zealand	16,60%
Norway	16,80%

!!!

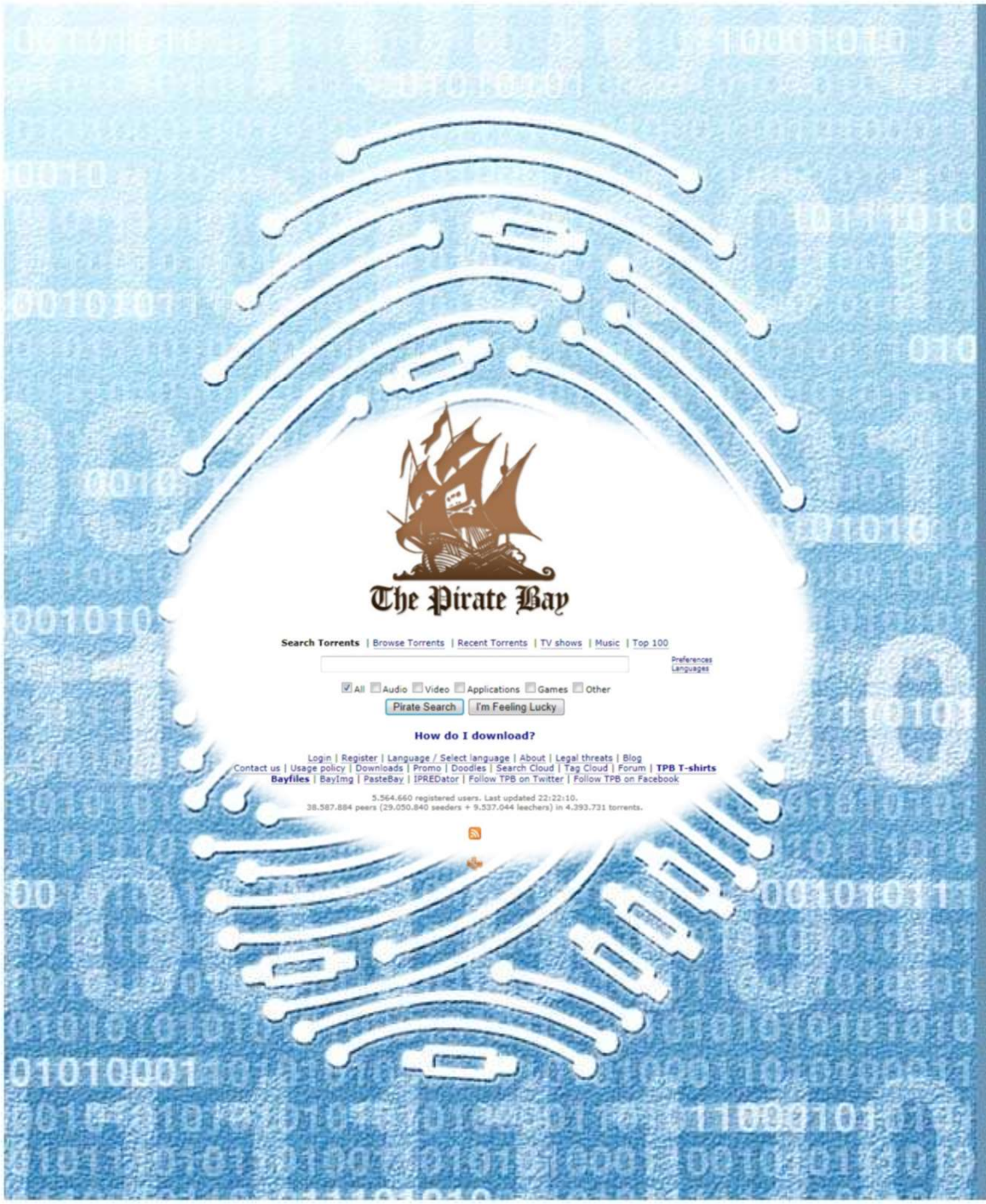
Osnovni preduslov za primenu zaštite je da rukovodstvo razume problem:

- **opasnosti koje mogu ugroziti informacioni sistem,**
- **uslove i ambijent koji pogoduju nastajanju neželjenih pojava, kao i**
- **moguće negativne (štetne) posledice koje zbog toga mogu nastupiti.**

!!! !!!

Rukovodioci su odgovorni za

- **zakonito,**
- **ispravno i pouzdano funkcionisanje IS i**
- **tačnost,**
- **ažurnost i potpunost podataka, pa samim tim i**
- **za zaštitu IS i podataka.**



3. PRAVNI I ETIČKI ASPEKTI ZAŠTITE

3.1. Jedinstvene osnove zaštite

3.2. Zaštita privatnosti

3.3. Zaštita intelektualne svojine

3.4. Sankcionisanje računarskog kriminaliteta

Kompjuterski crv Dorkbot se širi preko poruka na Skype-u

Vesti, 09.10.2012, 11:18 AM

Kompjuterski crv Dorkbot već je prevario mnoge korisnike Facebook-a i Twitter-a, a sada su na red izgleda došli i korisnici Skype-a.

Nekoliko proizvođača antivirusa upozorilo je na pojavu nove verzije crva koji se širi preko liste kontakata zaraženih korisnika Skype-a, šaljući poruku na engleskom (postoji i verzija teksta poruke na nemačkom) "Lol is this your new profile pic?".

Klik na link otvara .zip fajl koji sadrži fajl "skype_02102012_image.exe". Otvaranje .zip fajla rezultira instalacijom crva Dorkbot. Zaraženi računar tada postaje deo bot mreže, a crv ima i novu funkcionalnost, koja se prvi put pojavljuje u ovoj verziji - zaključavanje zaraženog računara sa zahtevom od korisnika da plati otkup otetog računara u roku od 24 do 48 sati. Suma koju otmičari traže iznosi 200 dolara.

Istoimeni malver širio se tokom poslednjih godinu dana društvenim mrežama Facebook i Twitter kao i preko chat kanala i USB fleš memorija. Ono što je novost je da nova verzija ima funkcionalnost ransomware-a.

Korisnici zaraženih računara vide obaveštenje u kome se tvrdi da je računar korišćen za nelegalne aktivnosti, kao što je dečija pornografija, odnosno pristupanje sajtovima sa ovakvim sadržajem ili krađa muzike koja je zaštićena autorskim pravima. Žrtvi se preti da će slučaj biti prijavljen vlastima ukoliko ne plati kaznu.

Trend Micro je juče objavio da je otkriveno nekoliko stotina zaraženih računara u različitim zemljama, ali to je još uvek mali broj zaraženih računara s obzirom da Skype koriste milioni ljudi.

Skype je reagovao na vesti o kompjuterskom crvu koji se širi preko ovog servisa a iz kompanije kažu da bezbednost shvataju veoma ozbiljno i savetuju korisnicima da preuzmu najnoviju verziju Skype-a i ažuriraju zaštitne funkcije na svojim računarima. Takođe, iz Skype-a upozoravaju korisnike da budu veoma oprezni sa neobičnim porukama čak i ukoliko takve poruke dolaze od prijatelja.

Piraterija i malveri: Zašto je besplatno ponekad najskuplje

Vesti, 11.10.2012, 08:35 AM

Napadi sa interneta su u porastu, ali rizici koje nosi pretraživanje interneta su zanemarljivo mali u o odnosu na opasnost koju predstavlja preuzimanje i deljenje nelegalnog softvera, video i muzičkih fajlova i drugih piratizovanih sadržaja.

U najnovijem Microsoft-ovom izveštaju (pdf) koji se bavi problemima bezbednosti, objavljenom u ponedeljak, upozoreno je na rastući trend infekcija čiji su izvor nebezbedni lanci snabdevanja, koji se u izveštaju definišu kao veb sajtovi, protokoli, i drugi kanali kojima se distribuiraju programi i drugi fajlovi.

Takozvani lanci snabdevanja uključuju veb sajtove sajber podzemlja, P2P mreže, kopije diskova i nepouzdane arhive softvera i druge nesigurne izvore.

Ponekad su žrtve napada potpuno nevine, kao na primer u sučaju preuzimanja besplatnih softverskih paketa za koje se ispostavi da kriju malver. Primera radi, u prvoj polovini ove godine istraživači Microsoft-a su otkrili 35 različitih vrsta malvera maskiranih u "install_adobeflash.exe".

Još češće se dešava da je malver upakovan u nelegalne kopije komercijalnog softvera ili medija koje preuzimaju korisnici koji žele da prođu što jeftinije.

Prirodno, iza ovih tvrdnji stoje interesi Microsoft-a. Microsoft-ov softver je među najčešće piratizovanim programima u svetu.

Da bi naglasili opasnost nelegalnog preuzimanja, Microsoft-ovi istraživači se u izveštaju posebno bave malverima i neželjenim programima koji su blisko povezani sa nelegalnim preuzimanjem.

Jedna takva porodica malvera je Win32/Keygen, što je generičko ime za kategoriju programa koji generišu licencne kodove za različite softverske pakete, kao što su MS Office, Photoshop i drugi. Tehnički, Win32/Keygen je potencijalno neželjeni program pre nego malver jer program iz ove kategorije nije nužno i nosilac štetnog koda. I druge porodice malvera kojima su se u izveštaju bavili istraživači Microsoft-a slede sličan obrazac. Neki služe za zaobilaženje procesa aktivacije MS

3. Pravni i etički aspekti zaštite

U informacionim sistemima skoncentrisana je ogromna količina

- filtriranih,
- proverenih i
- uređenih podataka i informacija

koji mogu da izražavaju materijalnu vrednost (na primer, „elektronski novac“ ili stanje robe u skladištu), ali isto tako mogu da predstavljaju ličnu, poslovnu, profesionalnu, bezbednosnu, vojnu ili državnu tajnu.

Činjenica je da računari brzo i sigurno preuzimaju brojne, pa i najvitalnije, funkcije ljudske delatnosti,

Društvo se ubrzano kreće pravcem koji ga vodi ka velikoj zavisnosti od ove tehnologije, i to u svim oblastima i na svim nivoima.

Pošto je u pitanju opštedruštveni interes, ovi problemi nisu prepušteni samo korisnicima informacionih tehnologija, već su postali opšte-društvena briga sa prioritetom najvišeg stepena.

Zbog ozbiljnosti, složenosti i značaja, zaštita informacionih sistema, a posebno njen pravni aspekt, je već godinama predmet studija, rasprava i odluka različitih nacionalnih i međunarodnih tela i organizacija, a broj zemalja koje su ovu materiju u manjoj ili većoj meri, na ovaj ili onaj način, regulisale – stalno se uvećava.

Ova društvena akcija, zbog specifičnih karakteristika problema, treba da ima preventivni i represivni karakter i da se odvija u više pravaca, od kojih su najvažniji prioriteti:

- **Jedinstvene osnove zaštite;**
- **Zaštita privatnosti;**
- **Zaštita intelektualne svojine;**
- **Sankcionisanje računarskog kriminaliteta.**

Sve ove oblasti čine jedinstvenu globalnu celinu – zaštita u oblasti IKT-a.

Полазећи од основног циља заштите информационих система, да се обезбеди и заштити интегритет и расположивост рачунарске опреме, као и интегритет, расположивост и тајност података и информација, могло би се констатовати да постојеће стање не задовољава и да у овој области предстоји још много тога да се уради.

Владе многих земаља, као и бројне професионалне и комерцијалне организације, асоцијације и институције улагале су и улажу велике напоре у циљу разрешавања проблема заштите аутоматизованих информационих система.

У области заштите информационих система вредна пажње на међународном плану је свакако и активност Организације за економску сарадњу и развој OECD (Organisation for Economic Cooperation and Development) и Савета Европе.

Jedinstvene osnove zaštite

- Postojeće stanje nije zadovoljavajuće i u ovoj oblasti predstoji još mnogo toga da se uradi.

- Ono što je potrebno svakako nisu samo suvoparni naredbodavni zahtevi, već niz uputstava, preporuka, smernica i standarda, u formi preporučenih procedura, sa rešenjima koja su:
  - Tehnički dostupna;
  - Troškovno prihvatljiva;
  - Fleksibilna;
  - Merljiva.

Kako se zaštiti od samog sebe

Prevara robom "neverovatnih" svojstava jedan od najvećih izvora nelegalne zarade na internetu.

- **Svake 44 sekunde neko postane žrtva, pošto se odluči da kupi robu za čije je "čudotvorne moći" čuo preko interneta**
- **1400 sumnjivih sajtova samo u oblasti zdravlja, što je rezultiralo podizanje tužbi protiv 18 kompanija i detaljnim istragama koje obuhvataju još 200 firmi u 19 zemalja širom sveta**
- **Na vrhu liste "svemogućih" proizvoda nalaze se pilule koje omogućavaju svjim korisnicima da piju piva koliko žele, a da se ne ugoje (cena 71 dolar za 60 tableta)**
- **Pojas, koji kada se nosi dok sedite u fotelji izaziva isti efekt kao 600 sklekova urađenih u 10 min.**
- **ljuske od jajeta ptice emu koje navodno povećavaju libico, tečnost koja masnoću iz tkiva tokom spavanja pretvara u mišiće,**

prevara.info

Društvo za borbu protiv prevare

www.prevara.info je vlasništvo *Društva za borbu protiv prevare*. Stranica se ažurira svakog ponedejlka, ali i danima kad se pojavi neka nova prevara. Ako želite da nam se pridružite i pomognete sebi i drugima, možete da to uradite putem email-a ili telefonom, a koji se nalaze u rubrici kontakt.
Budi drug. Obavestite ostale.

Poštovani novinari: Zaista nam je drago što ste našu ideju preneli u:novine, tv ili radio. Vapaj za borbu protiv prevare, stigao je i do policije i ministara... i mi smo Vam zahvalni za to. Samo Vas molimo da spomenete i nas. Ipak, zaslužili smo to. Zar ne?

Društvo za borbu protiv prevare se zahvaljuje: Radio Televizija Srbije (Beogradska hronika, Magazin Oko), Radio televizija Pink (Nacionalni Dnevnik), Radio televizija Vojvodine (Novosadske razglednice, Dobro jutro Vojvodino, Život je lep), Televizija Avala (Jutarnji program, U toku), Televizija B 92 (Vesti B92, Vesti B92 Info, Priči nikad kraja), Televizija Rubin Kikinda, Televizija Košava, Kurir (crna hronika), Građanski List, Ilustrovana politika, Blic, Revija D Crna Gora, Večernje novosti, Frankfurtske vesti, Borba, Glas javnosti, Nedeljni telegraf, Politika, Nin, Politika magazin, Tanjug, Magazin Kod, Ekonomist, Tabloid, Press, Akter, Danas, Vijesti, Alo, Radio B 202, Radio 021, Radio Kikinda, Radio Slobodna Evropa, Radio Hit Kragujevac, Radio s, Vesti, Forum Krstarice, Internet Novine Serbske, NS kafe.com, YU serach.com, MTS Mondo, Sezampro, Privredna komora Beograd ...za podršku u borbi protiv prevare...

Obaveštenje: ***Do sada smo objavili 384 prevare i objavljujemo nove svakog ponedeljka. Sve prevare možete naći u spisku prevara ili***

Novi sadržaji | Čitano

- Kako mogu da Vam oduzmu stan na prevaru
- Nepismena Nigerijska prevara
- Download video
- Nepoštene agencije za iznajmljivanje stanova
- Koliko i kako vredi garancija

KAKO NAPRAVITI NAJLEPŠU KAFU

3.2 Zaštita privatnosti

IT ima zadatak da:

- **prikupi,**
- **obradi,**
- **memoriše i**
- **distribuira,**

ogromnu količinu podataka i informacija, od kojih se veliki deo odnosi na podatke o ličnosti.

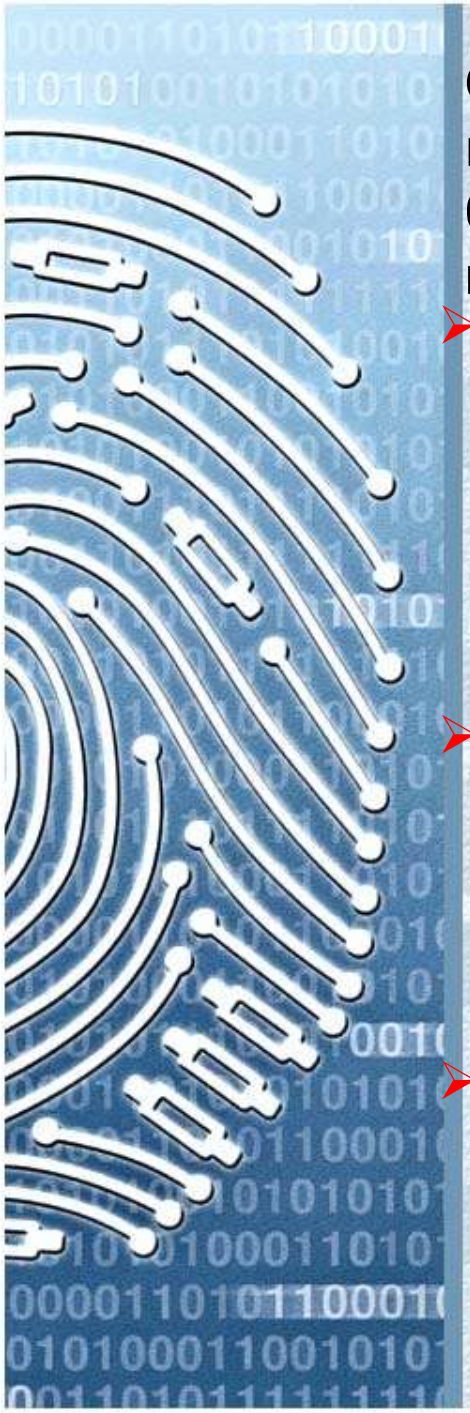
Ovim je problem privatnosti dobio sasvim nove dimenzije, pa je dijagnoza pravnika gotovo svuda ista: u automatizovanom ambijentu privatnost pojedinaca je ozbiljno ugrožena i potreban je odgovarajući sistem zaštite.

- **Privatnost je jedno od osnovnih ljudskih prava i kao takvo odnosi se na ona prava koja su vezana za ličnost čoveka, kojima se obezbeđuje integritet i dignitet ljudskoj ličnosti i koja zahtevaju očuvanje tajnosti i slobode privatnog života.**
- **Najprihvaćenija je koncepcija, po kojoj privatnost podrazumeva pravo pojedinaca da sami odrede obim ličnih informacija koje žele da dele sa drugima. Ona uključuje njihovo pravo da:**
  - **kontrolišu prikupljanje,**
  - **memorisanje i**
  - **diseminaciju**

  njihovih podataka ili informacija o njima samim.

  Ovaj vid privatnosti dobija i posebno ime – informaciona privatnost (information privacy).

- **Ovakav koncept priznaje pravo pojedincima da odobravaju i kontrolišu prikupljanje i korišćenje podataka o njima samim.**
- **Naravno, ovo pravo nije apsolutno i može, u strogo predviđenim slučajevima i okolnostima, od strane unapred određenih subjekata, biti „narušeno“.**
- **S druge strane, pravo na informacionu privatnost predstavlja kompleksno pravo koje obuhvata:**
  - **Pravo na obaveštenost;**
  - **Pravo na odgovarajuće korišćenje podataka;**
  - **Pravo pristupa i uvida;**
  - **Pravo ispravke;**
  - **Pravo na pravna sredstva.**



OECD је издао Смернице за заштиту приватности и међународних токова личних података. Смернице су базиране на осам основних принципа намењених за националну употребу:

- **Принцип лимитираног прикупљања података**

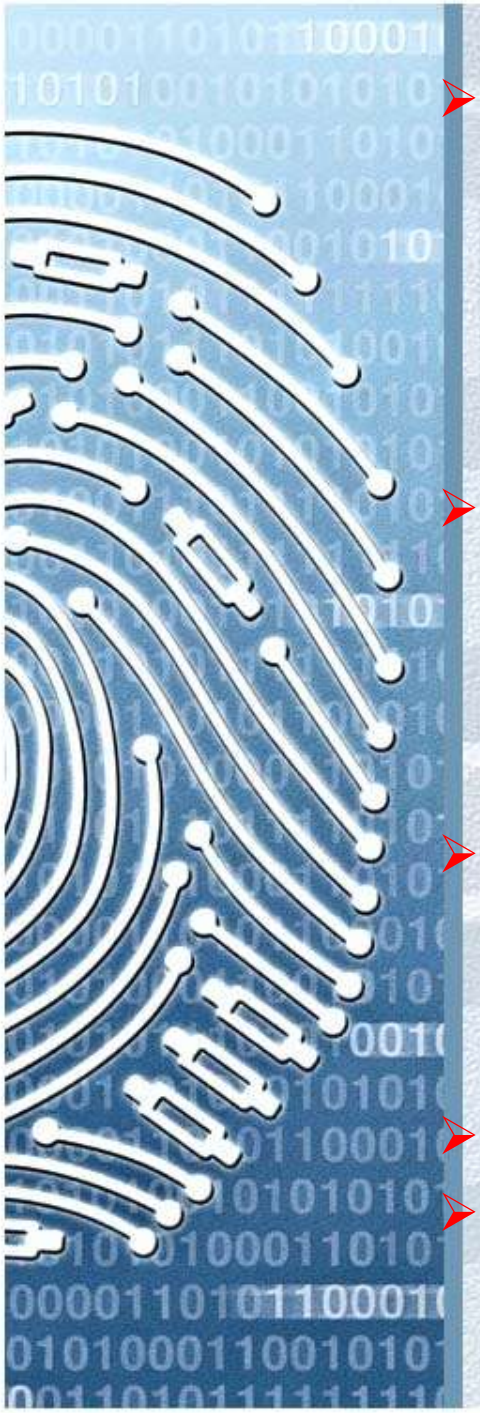
  мора да постоји ограничење за прикупљање личних података и да сви такви подаци морају бити добијени на законит и исправан начин и, где је могуће, са знањем и пристанком субјекта на којег се подаци односе.

- **Принцип квалитета података**

  Подаци о личности морају бити релевантни за потребе за које се прикупљају и у обиму неопходном за те потребе и морају бити тачни, комплетни и ажурни.

- **Принцип специфицирања потреба**

  Потребе због којих се подаци о прикупљају морају бити специфициране пре прикупљања , а њихово коришћење ограничено само на задовољење специфицираних потреба



- **Принцип ограниченог коришћења**

  Подаци о личности не би смели бити обелодањени, расположиви или коришћени за друге потребе које нису специфициране у складу са претходним принципом, изузев: уз сагласност субјекта или на основу законских овлашћења.

- **Принцип заштите**

  Подаци о личности морају бити заштићени разумним мерама од ризика губитка, неовлашћеног приступа, деструкције, коришћења, модификације или обелодањивања.

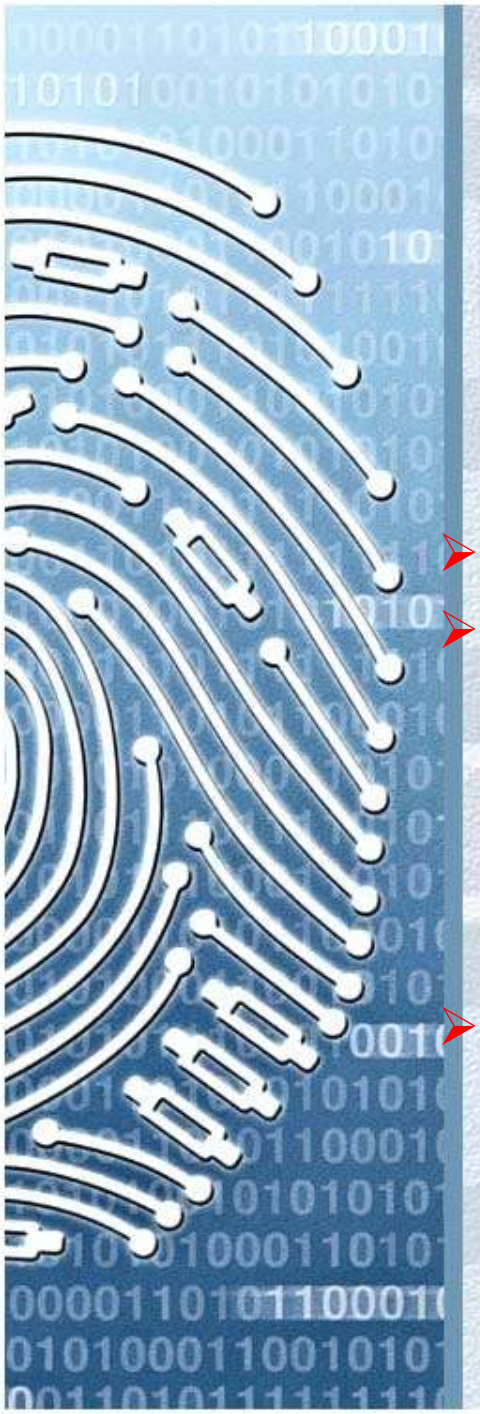
- **Принцип отворености**

  Мора да постоји генерална политика отворености развоја, праксе и политике у односу на личне податке.

- **Принцип индивидуалне партиципације**

- **Принцип одговорности**

  Подразумева одговорност контролора података за поштовање наведених принципа.



Савет Европе је 1980. године усвојио Конвенцију о заштити особа с обзиром на аутоматску обраду личних података. Кључне елементе Конвенције, који представљају минимум стандарда, а који би морали бити инкорпорирани у национална законодавства, чине ставови који се односе на следеће:

- **Квалитет података**
- **Посебне категорије података**: Подаци о личности који идентификују порекло, политичке ставове, религиозна или друга уверења, као и подаци о личности који се односе на здравствено стање, сексуални живот и криминалне активности, морају бити заштићени на адекватан начин.
- **Заштита података**: Одговарајуће мере заштите морају се предузимати према личним подацима смештеним у датотеке информационог система ради заштите од неовлашћене деструкције или инцидентног губитка, као и од неовлашћеног приступа, измене или дисеминације.

- **Додатна заштита за субјекте**: Свакој се особи мора омогућити да: **зна да су лични подаци о њој меморисани и за коју сврху**; у разумним интервалима и без превеликог закашњења или трошкова оствари увид у меморисане податке који се на њу односе; **тражи исправку погрешних података или брисање**, ако њихово меморисање није засновано на закону; има **могућност предузимања одговарајуће акције** (правног лека) ако претходно тражење није задовољено.
- **Изузеци и ограничења**: Изузеци су могући ако је у питању безбедност и одбрана земље, јавни ред, монетарни интерес државе, сузбијање криминалних делатности и заштита субјеката или права и слобода осталих субјеката.

Ова Конвенција је имала изузетан значај не само за земље чланице Европске уније, већ и за друге земље међу којима је и наша, која је 1992. године донела Закон о потврђивању ове Конвенције.

Стање код нас: С обзиром на чињеницу да је заштита података о личности једно од основних личних права грађана, у Уставу Републике Србије у члану 42 је истакнуто:

- **Зајамчена је заштита података о личности;**
- **Прикупљање, држање, обрада и коришћење података о личности уређује се законом;**
- **Забрањена је и кажњива употреба података о личности изван сврхе за коју су прикупљени, у складу са законом, осим за потребе вођења кривичног поступка или заштите безбедности Републике Србије;**
- **Свако има право да буде обавештен о прикупљеним подацима о својој личности и право на судску заштиту због њихове злоупотребе.**

Krađa identiteta najlakša preko JMBG

- Ljudi u Srbiji nisu svesni gde sve seju svoje lične podatke i ne znaju dovoljno o opasnostima da im neko ukrade identitet, kao i da će im se u tom slučaju život pretvoriti u zonu sumraka, kažu za „Blic” u kabinetu poverenika za informacije od javnog značaja.
- Rodoljub Šabić ističe da je u tom smislu najopasniji JMBG koji svi u svakoj prilici nekontrolisano dajemo, ne vodeći računa da na osnovu njega neko može da uđe u našu bazu podataka u poreskoj upravi ili u birački spisak i zloupotrebi.
- Što se tiče JMBG, već neko vreme se zalažem da promenimo taj broj i vežemo ga za neki promenljivi broj, a ne za nepromenljiva, jedinstvena svojstva ličnosti kao što su datum, mesto rođenja, pol. Mnoge zemlje su upravo zbog širokih mogućnosti zloupotrebe i nepromenljivosti ovog broja, odustale od njega, poput Hrvatske, a Portugalija ga je ustavom zabranila - objašnjava Šabić za „Blic

Sve češća krađa identiteta u Srbiji

IZVOR: 24 SATA

Beograd -- Poslednjih godina fenomen krađe identiteta sve prisutniji i u Srbiji. Procenjuje se da u Srbiji ima nekoliko stotina hiljada ljudi koji obrađuju lične podatke.

Ljudi u Srbiji nisu svesni gde sve ostavljaju svoje lične podatke i ne znaju dovoljno o opasnostima krađe identiteta. Najopasniji je jedinstven matični broj građana (JMBG) koji svi nekontrolisano dajemo ne samo policiji, bankama, zdravstvenim i obrazovnim institucijama, nego čak i prodavcima kada menjamo ili vraćamo kupljenu robu, piše list 24 sata.

Procenjuje se da u Srbiji ima nekoliko stotina hiljada ljudi koji obrađuju različite podatke o ličnosti. Iako se na krađu identiteta donedavno gledalo kao na stvar koja je rezervisana samo za ljude u zapadnim zemljama, poslednjih godina ovaj fenomen savremenog društva sve je razvijeniji i kod nas. "Važno je zaštititi privatne podatake i paziti kome ih dajemo, jer ne može baš svako da nam traži JMBG. Sve su češći primeri ljudi kojima na adrese stižu računi za razna dugovanja ili prijave za utaju poreza, u vezi sa poslovanjem preduzeća čiji su vlasnici, iako za njih prvi put čuju. Krađa identiteta i u Srbiji postaje sve unosniji posao", objašnjava poverenik za informacije od javnog značaja Rodoljub Šabić.

Najrobustnije krađe ličnih podataka ličnosti vezuju se za korišćenje savremenih tehnologija i upade u velike elektronske baze ličnih podataka kakve postoje u bankama, sistemima koji se bave e-trgovinom, ili kod nekih državnih institucija. Veliki problem, takođe, predstavljaju datoteke banaka i zdravstvenih institucija, kao i evidencija penzionih osiguranika. Posebnu poteškoću predstavlja zloupotreba ličnih podataka sa internet datoteka u svrhu marketinga, kao i krađa virtuelnog identiteta.

"Na osnovu JMBG-a koji internet korisnik neoprezno ostavi na nekom vebsajtu, može se ući u bazu poreske uprave ili birački spisak. Zahtev prodavaca građanima da im prilikom reklamacije ili vraćanja robe ostavljaju lične podatke je ne samo neetičan i neprihvatljiv, nego i očigledno nezakonit", objašnjava Šabić.

Mnoge zemlje su upravo zbog širokih mogućnosti zloupotrebe i nepromenljivosti ovog broja odustale od njega, poput Hrvatske, a Portugal ga je ustavom zabranio.

3.3. ZAŠTITA INTELEKTUALNE SVOJINE

Nesporno je da je računarski program rezultat stvaralačkih napora jednog ili više tvoraca. Zbog toga se isti i podvodi pod pravo intelektualne svojine kojim mu se osigurava zaštita, pre svega kao duhovnoj tvorevini, i čijim normama mu se, na nacionalnom i međunarodnom planu, obezbeđuje odgovarajući pravni tretman i omogućuje odgovarajući pravni promet.

Pravo intelektualne svojine obuhvata više oblika zaštite (patenti, autorsko pravo, poslovna tajna), ali je za zaštitu računarskih programa (aplikativni i sistemski programi – softver) danas najrasprostranjenije korišćenje autorskog prava.

http://www.kradimamu.com/

Kradi mamu - Zaštita intelektualne svojine na Internetu

Projekat oko koga su okupljeni svi oni kojima je stalo do poštovanja intelektualne svojine, sa akcentom na one na Internetu.

Prijavi lopova | Lopovi | Blog | O projektu | Kontakt

O projektu Kradi mamu

Svi koji se trude da redovno prate vesti u Srbiji ne mogu a da ne primete dugogodišnji pad kriterijuma takozvanih profesionalca u srpskom novinarstvu. Pored manjkavog sadržaja, redovne pojave bajatih „novosti“ i teškog manjka istražnog novinarstva, tu je i besramno nepoštovanje osnova novinarstva i novinarske etike (inače dva neizostavna predmeta na odseku za Novinarstvo visokoobrazovnih institucija u toj oblasti).

Sa pojavom građanskog novinarstva (citizen journalism) i veoma kompetentnih blogera i na našim prostorima, veliki broj „novinara“ je dozvolio sebi tu slobodu da direktno prepisuje ili preuzima, najčešće u celosti, ono što „amateri“ vredno sakupljaju, istražuju, kreiraju i postavljaju na svojim Internet stranicama. Ova pojava je sve češća, skoro normalna, i predstavlja ništa drugo do krađe intelektualne svojine. Profesionalni novinari se više ne ustručavaju da pokradu originalne tekstove i fotografije sa blogova ili drugih sajtova i bez obaveštenja, pitanja ili dozvole vlasnika ih objavljuju kod svojih poslodavaca. Što je najgore, te ukradene radove potpisuju svojim imenom i prezimenom, a i oni i njihovi poslodavci, objavljivanjem tih

Poslednje prijave

JužnaSrbija.info
mojgadget.net
Narodne novine Niš
besplatansport.com
Namestaj.rs Media Publishing Group

Poslednji komentari

mojgadget.net
Pozdrav! Oprostite, nisam posjećivao ovu...

JužnaSrbija.info
Aleksandre, imamo kopije svih mailova koji su...

JužnaSrbija.info
У име редакције: сајт је отвореног типа,...

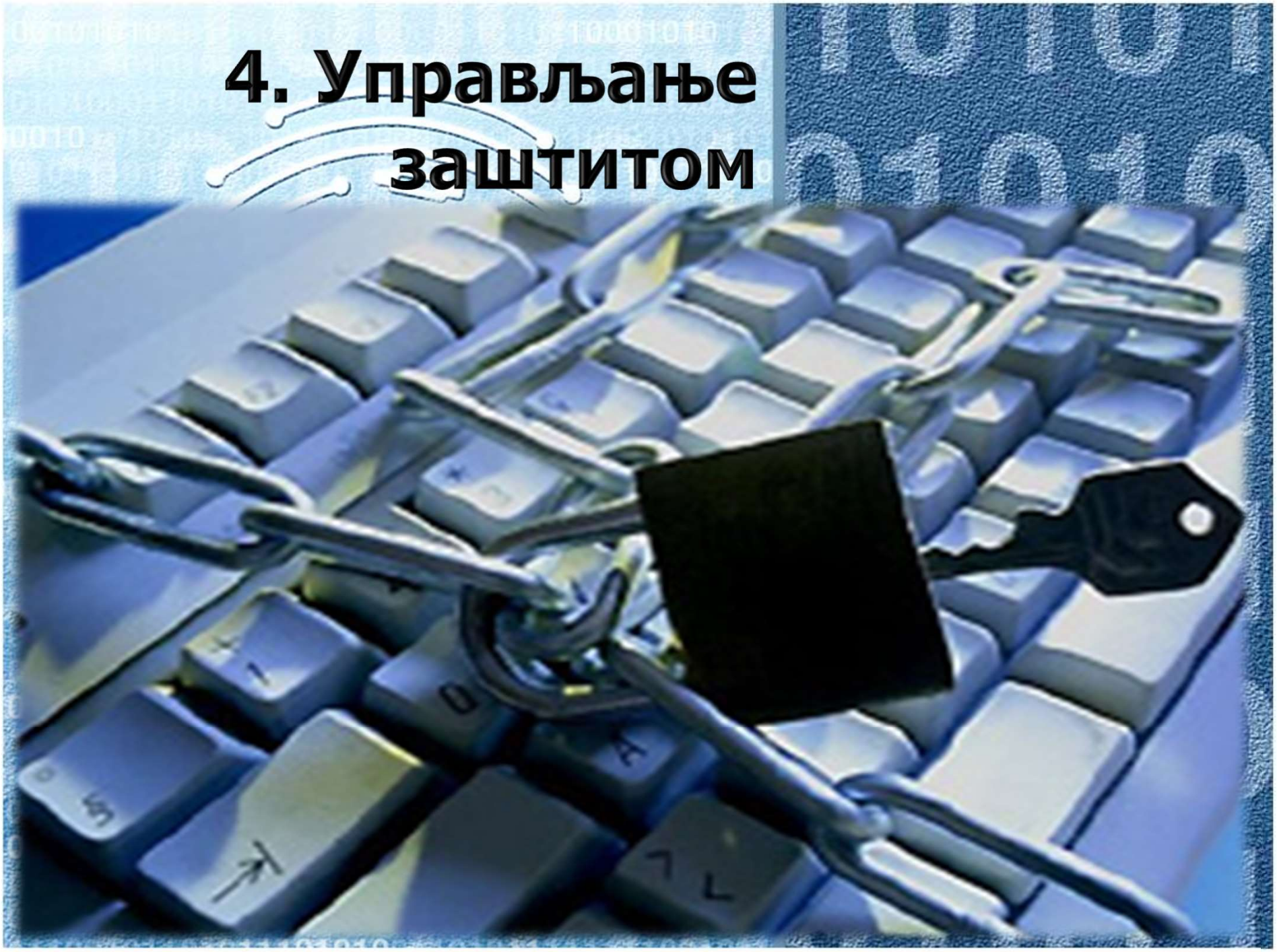
mojgadget.net
I dan danas ovaj članak nije obrisan, niti je...

mojgadget.net
U tom slucaju razumijemo ali vas molimo da...

Table 1.2
The Changing Nature of Theft

Older Manifestations of Theft	Modern Manifestations of Theft
Larceny and burglary (because property usually held on site)	Identity Theft (usually to gain access to the credit line/purchasing power of the owner)
Real property theft (cash, physical property)	Intellectual property theft (patents, trademarks, trade secrets, and copyright)
Pickpocketing and purse snatching (because property and cash often carried by individuals)	Skimming (theft of credit card information by deception, usually via electronic means) or Phishing (false e-mail solicitations to lure a suspect to divulge personal or credit information)
Risk higher (always the possibility of a face-to-face confrontation with the victim and the need to escape quickly from the crime scene to avoid apprehension)	Risk lower (never involves face-to-face contact with the victim, and no need for speed or agility because success requires deception rather than stealth)

4. Управљање заштитом



- **Управљање заштитом је организационо, стручно и технички врло сложен процес.**
- **Планирање, реализација и спровођење заштите се одвија истовремено са планирањем, увођењем и функционисањем информационог система.**
- **Развија се паралелно са развојем информационог система и траје дуже од самог информационог система (рокови чувања података и информација).**
- **Највећи део система заштите, посебно у делу планирања и увођења, реализују стручњаци специјалисти у сарадњи са произвођачима опреме и софтвера.**

Без улажења у уско стручну материју из области заштите информационих система и података, указаћемо на поједине сегменте који су значајни за профил стручњака који се школују на овом факултету, а то су :

41. **Анализа ризика;**
42. **Објекти које треба штитити;**
43. **Могуће претње – опасности;**
44. **Могуће последице;**
45. **Мере заштите; и**
46. **Политика заштите.**

4.1. Анализа ризика

Анализа ризика је начин обезбеђивања објективно заснованог приступа процени и управљању ризиком.

Омогућава:

- **идентификацију потенцијалних губитака који су неприхватљиви за дати систем и**
- **избор ефикасних и делотворних мера заштите.**

За обављање анализе ризика на располагању су бројне методе и технике које се међусобно разликују по

- **природи,**
- **ширини и**
- **дубини обухвата.**

- **Реч је о процедури која се користи за процену вероватноће претњи и потенцијалног губитка.**

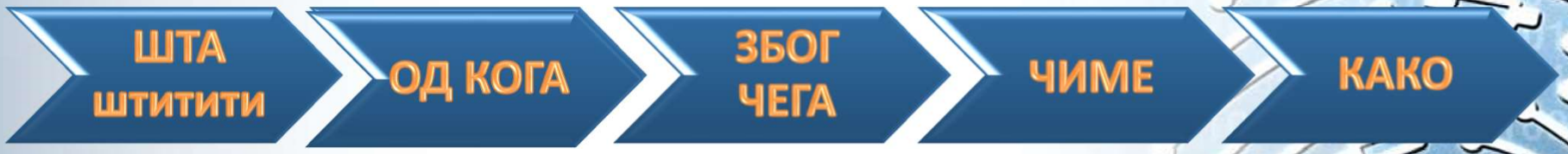
4.2. Објекти које треба штитити

1. КЉУЧНИ КОРАК

Један од основних критеријума је вредност за онога коме припадају. У том смислу наведен је један скуп типичних објеката:

- **Подаци**
- **Датотеке**
- **Базе података**
- **Софтвер**
- **Програми**
- **Централна јединица**
- **Периферни уређаји**
- **Екстерне меморије**
- **Терминали**
- **Персонални рачунари**
- **Листинзи**
- **Документација**
- **Локације за смештај**
- **Инфраструктура**
- **Комуникациона опрема**

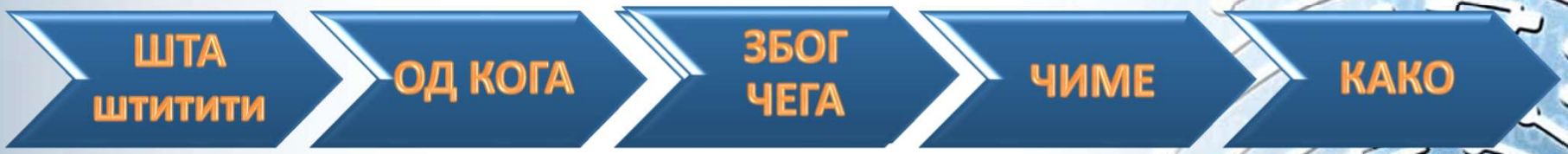
4.3. Могуће претње – опасности



- **Информациони системи су подложни свим класичним ризицима, као што су ватра, вода, експлозија и др., али и специфичним, као што су компромитујуће електромагнетно зрачење (КЕМЗ), рачунарски криминал и друго.**
- **Одређену тешкоћу представља и чињеница да је број претњи које могу угрозити информациони систем практично неограничен, због чега их је и немогуће све предвидети.**
- **Често се претња која није била ни идентификована покаже катастрофалном**

“Виша сила”	Хардверско-софтверски недостаци	Људски фактор
➢Земљотрес ➢Олуја ➢Поплава ➢Пожар ➢Висока температура ➢Нестабилност напајања ➢Електромагнетна зрачења ➢Ванредне прилике ➢Ратно стање	➢Кварови на информатичким уређајима ➢Техничка грешка инфра-структуре ➢Грешке у контролним или управљачким програмима ➢Грешке у апликативним програмима	**са атрибутом ненамерности** ➢Нехат ➢Нестручност ➢Недисциплина ➢Лоша организација ➢Замор **са атрибутом намерности** ➢Нарушавање приватности ➢Одавање тајне ➢Проневере ➢Саботаже ➢Фалсификовање ➢Стварање и дистрибуција вируса ➢Електронско узнемиравање ➢Крађа рачунарских услуга

4.4. Могуће последице



Одговор на ово питање представља уствари утврђивање негативних (штетних) последица које идентификоване претње могу изазвати

Постоје бројне могућности приступа класификацији негативних последица.

- **Делимично или потпуно физичко оштећење;**
- **Отуђење;**
- **Модификација;**
- **Успоравање радног процеса;**
- **Потпуна или делимична, дужа или краћа обустава радног процеса;**
- **Компромитација тајности.**

Глобално гледајући, наведене последице би се уопштено могле исказати кроз нарушавање:

- Интегритета;
- Расположивости;
- Поверљивости.

Интегритет се користи у контексту тачности и комплетности информација

Систем, да би се сматрао расположивим, мора бити на месту и употребљив за обављање намењених му функција. У том контексту термин „расположивост“ повезан је са континуитетом услуга.

Поверљивост се користи у контексту осетљивости на откривање (обелодањивање) података и информација.
При томе треба имати у виду да у неким случајевима осетљивост укључује и степен временске зависности.

4.5. Мере заштите

Идентификација свих мера које стоје на располагању.
Све те мере, по својим природним својствима која их карактеришу, могу се разврстати на следећи начин:

- **Нормативне;**
- **Физичко-техничке;**
- **Логичке;**
- **Криптолошке.**

Оваква класификација расположивих мера омогућава навођење њихових, са становишта ефикасности и трошкова, најбитнијих карактеристика, које могу послужити као врло поуздани критеријуми приликом њиховог избора.

4.6. Политика заштите

Одговор на ово питање уствари представља дефинисање политике заштите која ће се спроводити у конкретном амбијенту.

Треба имати у виду да је циљ налажења одговора уствари утврђивање свих релевантних фактора и њихових међусобних веза, неопходних за један, због њихове променљивости у времену и простору, циклични процес познат под називом „Управљање (овладавање) ризиком (променама, неизвесношћу или кризом)“, који подразумева спектар активности (укључујући нормативне, физичко-техничке и логичке контроле и процедуре) и којим се савлађује рањивост информационих система.

Основни циљеви управљања ризиком су:

- **Заштита система од губитака** који би угрозили његову могућност достизања циљева због којих је дизајниран, развијен и имплементиран;
- **Смањење на минимум** очекиваних **трошкова** предузимања адекватних мера заштите;
- **Смањење на минимум губитака** изазваних претњама које су се реализовале и поред предузетих заштитних мера.

Тежиште акције, није на елиминацији ризика, већ на управљању ризиком.

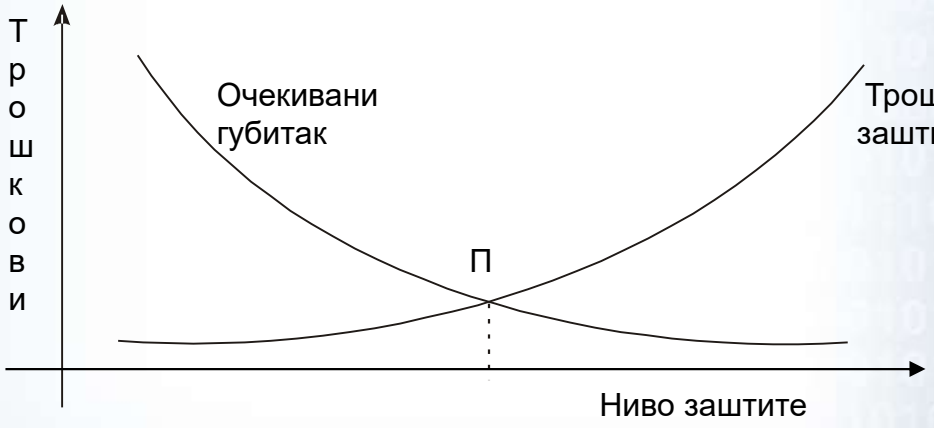
У пракси би ово значило да је неопходно:

- **Разумети природу и озбиљност различитих типова ризика којима је информациони систем изложен;**
- **Одредити ниво ризика који се може сматрати прихватљивим у амбијенту у којем систем функционише, с обзиром на обим ресурса који се морају утрошити, било у форми ризиком изазваних губитака или у форми издвајања за неопходне мере заштите;**
- **Редуцирати селекцијом, применом и имплементацијом одговарајућих и трошковно прихватљивих мера, постојећи ризик на ниво који се може сматрати прихватљивим или бар оправданим.**

Улагања у заштиту морају бити у складу са вредношћу објеката који се штите

Трошкови заштите не би смели бити ни већи ни једнаки потенцијалном губитку. !!!

Однос потенцијалног губитка и трошкова заштите графички је приказан на следећој шеми. Пресек кривих (тачка П) означава оптимални ниво заштите.



- Želim Vam puno uspeha u savladavanju gradiva!

- Za sva dodatna pitanja možete koristiti kontak adresu

tanja.kaurin@flv.edu.rs