Bezbednost informacija
Fakultet bezbednosti

dr Ana Kovačević

kana@rcub.bg.ac.rs

Uvod

- Intenzivan razvoj ITa
- Velika količina digitalnih podataka
- Problem: bezbednost računara, mreža i podataka

Bezbednost informacija

Cilj ovog predmeta jeste da studente upozna sa raznim aspektima bezbednosti informacija i informatičkih resursa, kao i sa važećim standardima u ovoj oblasti

Ocenjivanje

Način ocenjivanja:

- Predispita obaveza (Seminarski rad): max 20 poena VAŽI godinu dana: predati do 2.4.2019.

- Aktivnost na času (10 poena): domaći
- Seminarski 20 poena
- Ispit (pismeno): max 70 poena
- Ocena = predispitne obaveze+poeni na ispitu (>50%).

Ocenjivanje

$0 \leq$ broj poena < 51	5
$51 \leq$ broj poena ≤ 60	6
$61 \leq$ broj poena ≤ 70	7
$71 \leq$ broj poena ≤ 80	8
$81 \leq$ broj poena ≤ 90	9
$91 \leq$ broj poena	10

Konsultacije

- SREDA od 17.30-18.30
  - Uz prethodnu najavu mailom

Literatura

- Predavanja
- Chuck Easttom:Computer Security Fundamentals, 2016
- Pleskonjić i dr., Sigurnost računarskih sistema i mreža, Mikroknjiga 2007
- www.informacija.rs
- https://www.schneier.com/
- Kukrika Milan: Upravljanje sigurnošću informacija – Zaštita informacionih sistema prema standardu ISO 17799, INFO Home, Beograd, 2002.
- Standardi:
  - **SRPS ISO/IEC 27001**
  - **SRPS ISO/IEC 27002**
- **Itd**

Malver za rudarenje kriptovalute pronađen u 19 aplikacija iz Google Play prodavnice

Mobilni telefoni, 14.02.2018, 01:00 AM

Istraživači britanske kompanije Sophos otkrili su 19 Android aplikacija koje su se našle u Google Play prodavnici a koje su krišom učitavale Coinhive skriptu bez znanja korisnika.

Veruje se da je ista osoba ili grupa autor svih ovih aplikacija. Oni su sakrili Coinhive JavaScript majning kod u HTML fajlove u folderu apps/assets.

Maliciozni kod se pokreće kada korisnik pokrene aplikaciju i aplikacija otvara WebView.

U nekim slučajevima, u kojima aplikacija nije otvorila WebView, ova komponenta je bila sakrivena i rudarenje se odvijalo u pozadini.

U drugim slučajevima, u kojima je aplikacija bila čitač vesti ili tutorijala, Coinhive in-browser majning kod se pokretao sa legitimnim sadržajem aplikacije dok je aplikacija korišćena.

Izdvojeno

Android 9 protiv spywarea: Novi Android OS će blokirati aplikacijama pristup kameri u stanju mirovanja

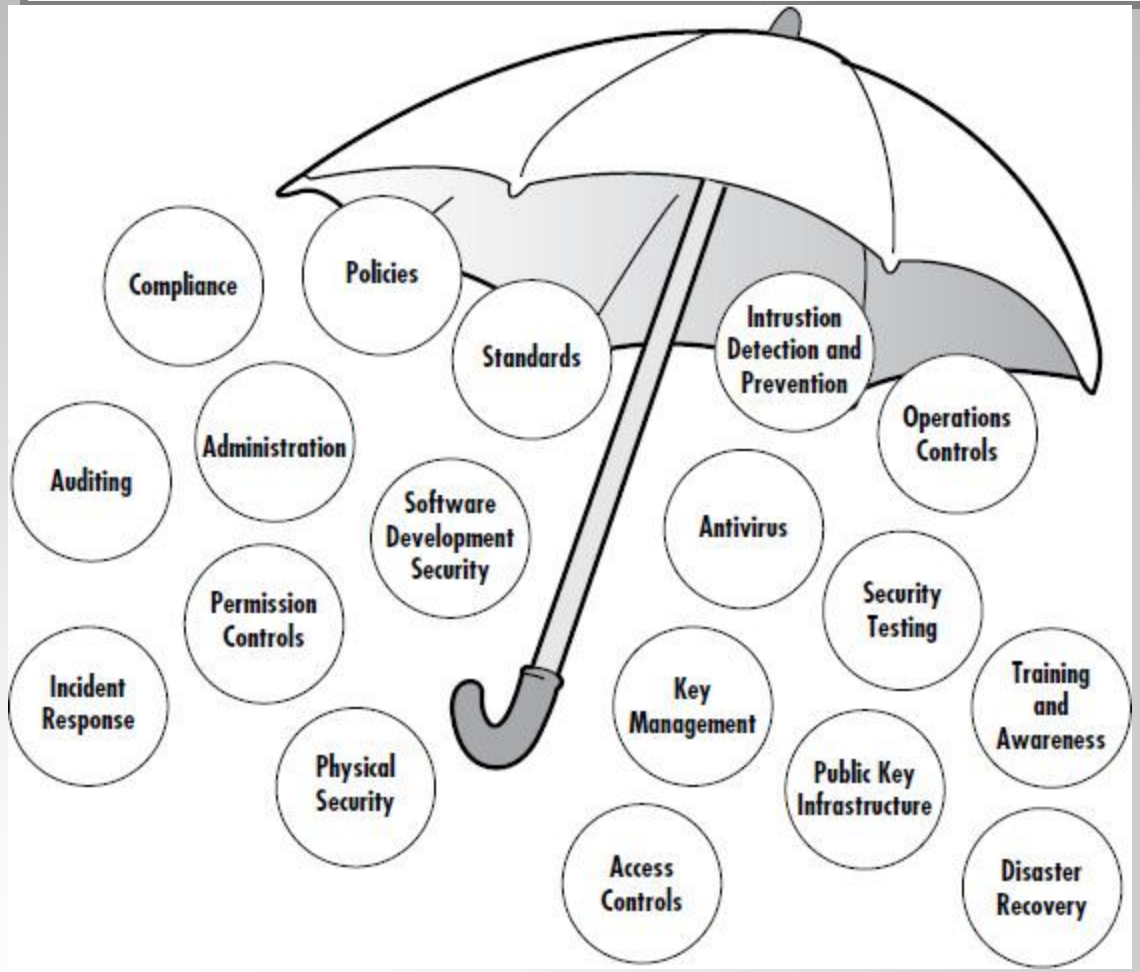
Googleov naredni operativni sistem za mobilne uređaje Android 9 (Android P) doneće mnogo novih

1 Predavanje: UVOD

Bezbednosni izazov

- Primena računara u svim oblastima života => veliki broj podataka.
- Eksplozivni razvoj Interneta i servisa za plaćanje putem Interneta.
- **Računari kao oružje, kao podrška poslu, ali i za kršenje zakona.**
- Bezbednosni proboj preko Interneta su u porastu, i računarski kriminal je u porastu.
- **Računarski kriminal (**ili visokotehnološki kriminal, sajber kriminal) obuhvata aktivnosti tokom kojih se računari, računarske mreže ili računarski podaci koriste kao izvori, sredstva, objekat ili mesta izvršenja krivičnog dela" (Milosavljević i dr., 2009).
- Kako učiniti računare bezbednijim?

Bezbednost informacija



Neophodnost multidisciplinarnog pristupa

Izvor: Information security: principles and practices, Merkow; Breithaupt 2014.

Apsolutna bezbednost ne postoji

- “The only secure computer is one that is turned off, locked in a safe, and buried 20 feet down in a secret location—and I’m not completely confident of that one, either” (Schneier 1995).

Bezbedbnost – smanjenje rizika

- Sa porastom računarskog kriminala – bezbednost značajna.
- **Bezbednost se odnosi na zaštitu računarskih sistema i podataka protiv neželjenog pristupa, oštećenja, modifikacije ili uništavanja.**
- Primena različitih računarskih tehnika da zaštite svoje sisteme: od jednostavne fizičke blokade do naprednih tehnika koje koriste kriptološke sisteme (šifre) i biometerijske podatke.

Bezbednost

- je objektivno stanje zaštićenosti računarskog sistema primenom:
  - upravljačkih mera (zakon, standardi, politika zaštite)
  - organizacionih mera (personalna, fizička zaštita, upravljanje incidentnom i vanrednim događajem, administracija sistema zaštite itd.)
  - tehničkih mera (kriptozaštita, logička kontrola pristupa, antivirusni programi, firewalls, IDS/IPS, skeneri itd.)

Informacija

- Digitalno doba
- Informacije predstavljaju određenu imovinu, imaju vrednost i potrebno da se adekvatno zaštiti.
- Bezbednost informacija obezbeđuje zaštitu od širokog opsega pretnji kako bi se osigurao kontinuitet poslovanja, min. gubici i max dobitak.

CIA vs DAD

- Tri fundamnetalna principa **bezbednosti informacija:**
  - Poverljivost (engl. Confidentality) informacija je dostupna samo onima koji su ovlašćeni da joj pristupe.
  - Integritet, celovitost (engl. Integrity) podatke ne smeju da menjaju neovlašćenja lica ili procesi;
  - Raspoloživost (engl. Availability) ovlašćeni korisnici mogu pravovremeno da prisutupe podacima ili računarskim resursima.
- SUPROTNO:
  - DAD Disclosure (otkrivanje), Alteration (izmena), Destruction (uništenje).

Poverljivost

- Poverljivost potiče iz svojinskih odnosa i značaja podataka za određene subjekte, a pretpostavlja da se poverljivi podaci ne smeju otkriti od strane neautorizovanih pojedinaca i organizacija ili u neovlašćenim procesima.
- Poverljivost – osobina da informacija nije na raspolaganju, niti dostupna onima koji nisu ovlašćeni da je prime.

Raspoloživost

- Raspoloživost = (stvarno vreme kada je sistem bio raspoloživ)/(vreme koje bi sistem trebao da bude raspoloživ)
- Npr. procenat vremena u kojem je najbliži terminal raspoloživ – dostupan za upotrebu (nije van upotrebe ili zauzet od strane drugog korisnika).
- Osiguranje raspoloživosti: sprečavanje odbijanja usluga.
- Raspoloživost: 1. zahtev (Kukrika, 2002).

Raspoloživost

- Raspoloživost podataka osigurava da im se može pristupati bez ograničenja i da se mogu slobodno koristiti kad je to potrebno.
- Da bi se ispunila raspoloživost treba obezbediti:
  - pravovremenost (pretnja je kašnjenje)
  - kontinuitet pružanja usluge (pretnja je odbijanje usluge)

Integritet

- Integritet treba ispuniti zahtev za korektnošću, kompletnošću (brisanje, dodavanje), validacijom i proverom autentičnosti.
- Tj. **da podaci nisu izmenjeni ili uništeni na neovlašćeni način.**
- Integritet se može posmatrati iz dve perspektive:
  - **integritet podataka** (osobina koja garantuje da podaci neće biti izmenjeni na neautorizovan način prilikom arhiviranja, procesiranja ili prenosa)
  - **integritet sistema** – kvalitet koji sistem poseduje dok obavlja zahtevane funkcije na besprekoran način, zaštićen od bilo kakve neautorizovane manipulacije).

PRINCIPI BEZBEDNOSTI

Uvod

- Najbolji specijalisti iz bezbednosti kombinuju praktična znanja i tehničke veštine sa razumevanjem ljudske prirode.
- Ne postoje dva sistema ili situacije koje su identične, i ne postoji priručnik koji rešava sve probleme bezbednosti.

Primer (info)

- 2003, Manchester (UK): Whitworth Gallery: Van Gogh, Picasso, Gaugain…(>$7mil)
- Zaštita: CCTV, alarmi, 24h obilaze patrole.
- April 2003, “kradljivci” upadaju u muzej, zaobilaze nivoe bezbednosnog sistema, i uzimaju 3 remek dela.
- Nakon par dana, slike su otkrivene u obližnjem restoranu sa porukom: “Naša namera nije bila da ukrademo, već da pokažemo slabost sistema”.

Princip 1

- Ako ima dovoljno vremena, alata, veština i sklonosti, zlonamerna osoba može da probije bilo koje bezbednosne mere.
- Bezbednosna testiranja omogućavaju dodatno vreme pa napadači mogu da se otkriju.

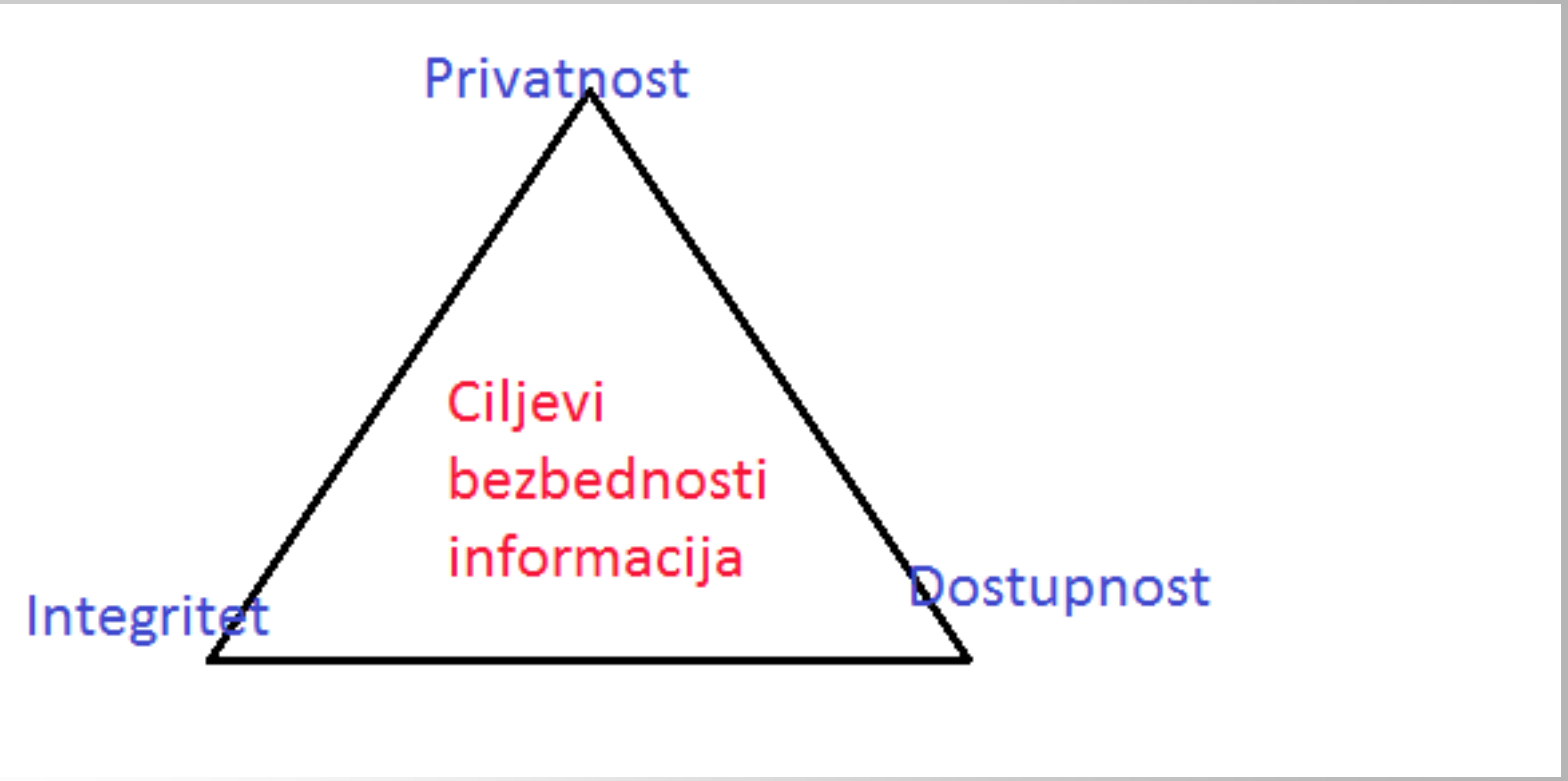
Primer: sefovi

- Sefovi su podeljeni u kategorije prema tome koliko dugo mogu da izdrže pre nego što ih provalnik otvori:
  - B-XXX: bilo koji kutija sa bravom; XXX debljina čelika; nisu testirani.
  - C-XXX. 1inch debela vrata, nisu testirani
  - UL TL-15: prošli su stanardizovane testove prema standardu UL Standard 687; preko 50 različitih tipova napada je isprobano, vreme 15min.
  - UL TL-30: slično kao UL TL-15, sem za što je vreme 30min i par alata više, i istraživači su imali i prospekt sefa.
- Nijedan sef nije apsolutno bezbedan, bezbednosne mere samo kupuju vreme.

Princip2: Tri bezbednosna cilja

- Tri osnovnva cilja bezbednosti informacija su: Privatnost, Integritet i Raspoloživost.
- Sve mere bezebednosti informacije obezbeđuju bar jedan od tri cilja: privatnost, integritet i raspoloživost (dostupnost).

CIA trougao


Privatnost
Ciljevi
bezbednosti
informacija
Integritet
Dostupnost

Integritet ciljevi:

- Obezbediti da neautorizovani korisnik **ne** izmeni podatke ili program.
- Obezbediti da autorizovani korisnik **ne** napravi neispravnu ili neautorizovanu modifikaciju.
- Održavati internu i eksternu konzistentnost podataka i programa.

Primer: raspoloživost- izazovi:

- DOS (Denial of Service)– prema namernom napadu ili zbog neotkrivenih mana u implementaciji.
- Gubitak mogućnosti IS zbog prirodnih nepogoda.
- Kvar na opremi tokom “normalnog” korišćenja.

Princip3: Strategija zaštite po dubini

- Primer: Do sefova u banci postoji nekoliko nivoa zaštite (čuvari, zatvorena vrata sa spec. pristupom).Soba sa sefom, može se pratiti sa CCTV, senzorima na pokret, alarmima koji otkrivaju neuobičajenu aktivnost. Zvuk alarma može zatvoriti vrata automatski, obavestiti policiju ili ispuniti sobu suzavcem.
- **Zaštita po dubini: štiti, otkriva i odgovara na napade na sistem.**

Princip3: Strategija zaštita po dubini

- Zaštita po dubini
  - Uključuje implementiranje bezbednosti u preklapajuće nivou što obezbeđuje tri elementa potrebna za osiguranje imovine: prevencija, detekcija i odgovor.
  - Slabosti jednog nivoa bezbednosti se može kompenzovati snagom drugih.

Phishing

- Phishing opasna Internet prevara
- Koriste se podaci dostupni iz socijalnih medija i omogućava zlonamernoj osobi da napravi profil žrtve da bi ga bolje ubedila da je prevara realna.

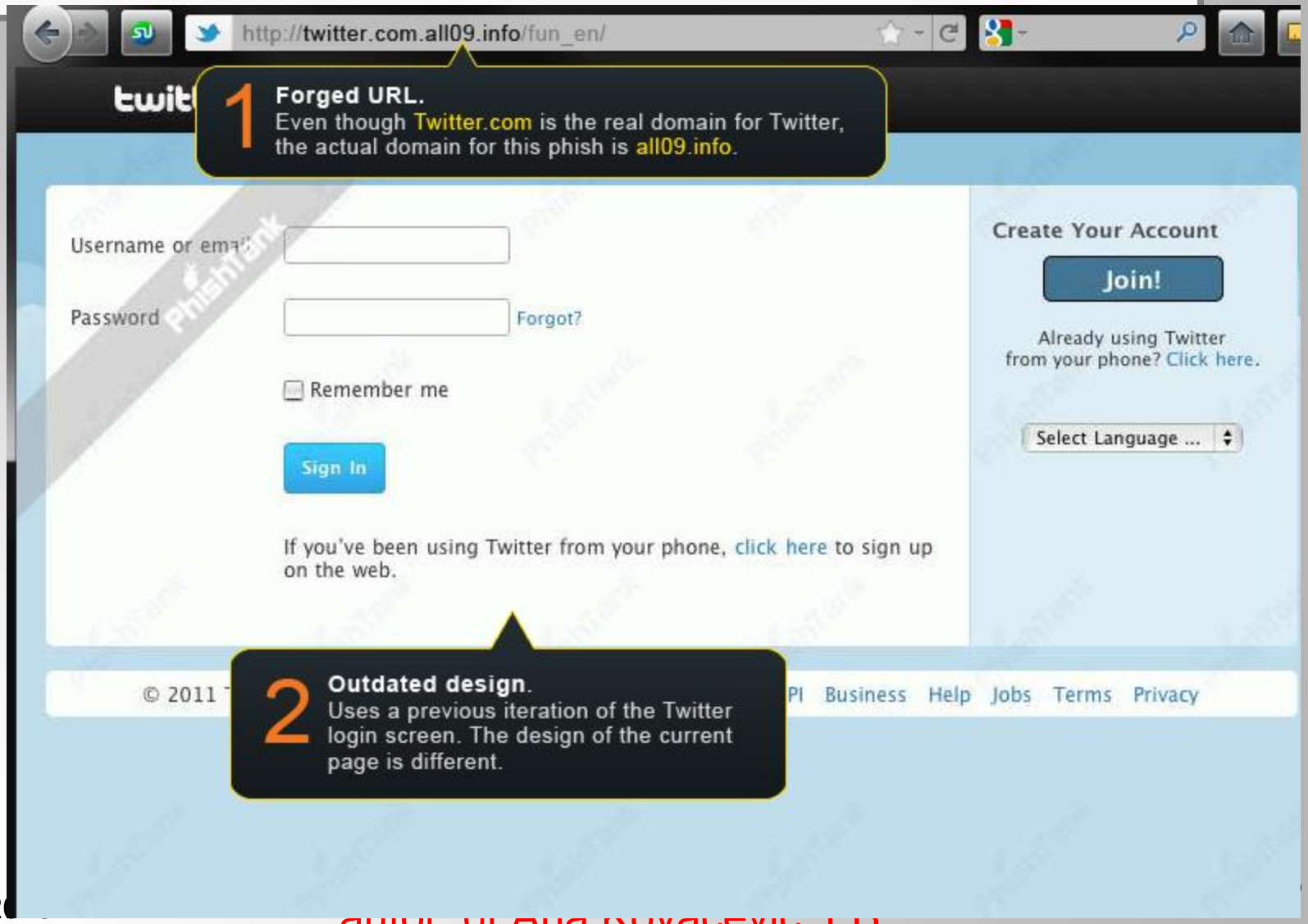
Phishing-primer

1. Žrtva prima naizgled poslovni mail koji je stigao od “sigurnog” izvora, kao onlinebanking sajta ili…
2. U emalu stoji da je neophodno da se ažurira nalog odmah ili će biti suspendovan na nekoliko dana.
3. Email sadrži URL (link) i upućuje korisnika da klikne na link i ažurira informacije. Tekst linka kao za očekivani sajt, no link je veza do napadačevog sajta (koji je napravljen da izgleda kako korisnik očekuje da vidi).
4. Na lažnom sajtu, korisnik unosi ID/password
5. Sajt javlja uobičajenu poruku npr. “We’re sorry- we’re unable to process your transaction at the time”
6. Žrtvini podaci su kod napadača koji može njima da se koristi.

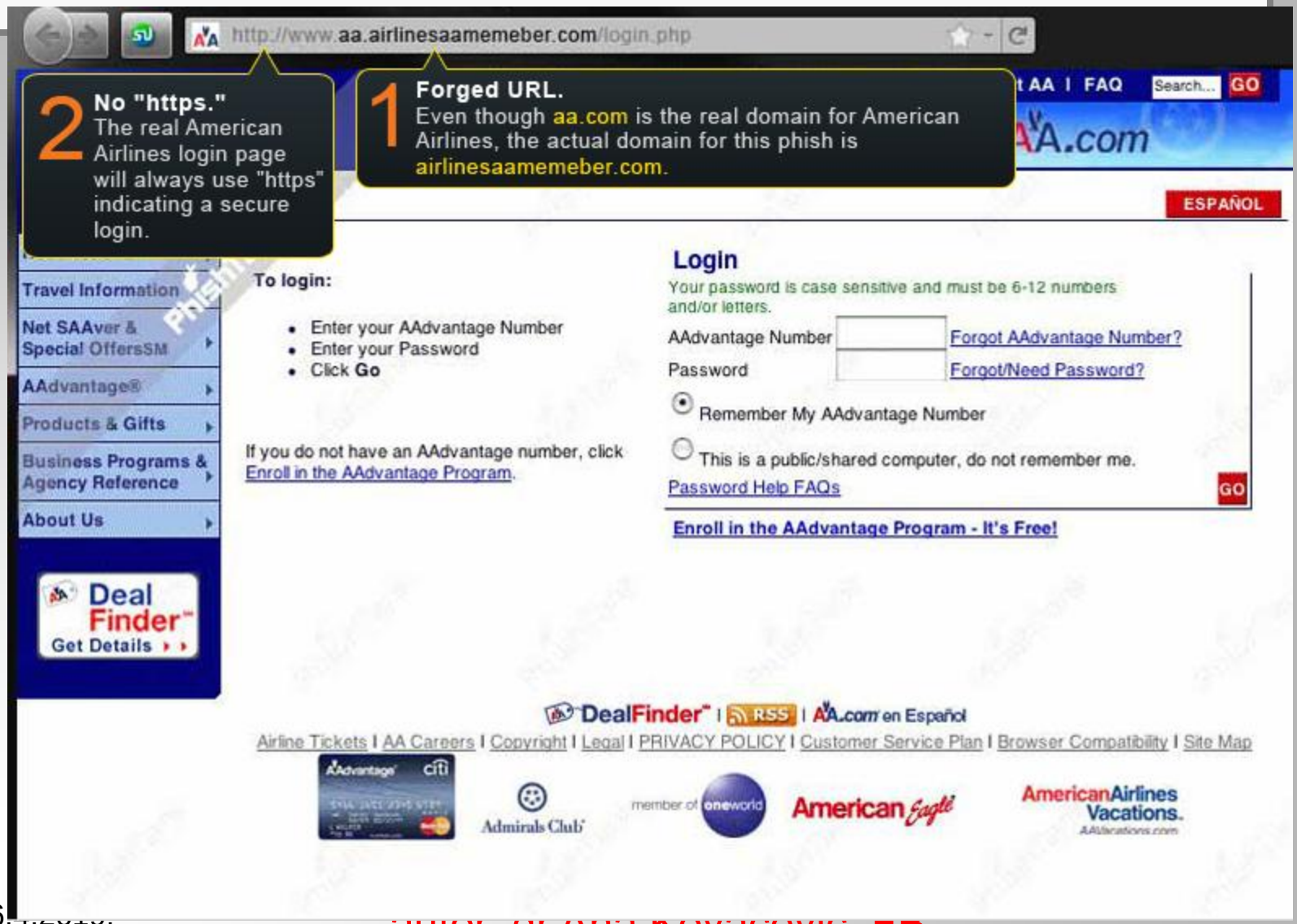
Zaštita od phishinga

- “Osvešćavanjem” i edukacijom
- Uočiti znakove prevare: phishing mail umesto imena koristi *User* ili na osnovu email adrese;
- Nikada ne kliknuti na linkove u netraženim finansijskim mailovima. Iako link izgleda regularan on vodi do sajta napadača.
- Proveriti prijavljivanje na regularan sajt.
- Proveriti sa vašim provajderom (organizacijom, bankom…) vezano sa phishing prevare za koje znaju.

Primer: Phishing



Primer: Phishing



4 princip: Kada su prepušteni sami sebi ljudi prave najlošije "bezbednosne odluke"

- Malo je potrebno da se ubedi pojedinac da se odrekne poverljivih informacija u zamenu za beznačajnu ili bezvrednu robu.
- Primer: Infosecurity Europe (UK najveće IT izložba bezbednosti): istraživači na stanici Waterloo su dobili poslovni pw za olovku; ¾ je odmah odalo, a 15% nakon kratkog ubeđivanja.
- Mnoge ljudi je jednostavno ubediti da dvosturko kliknu u attachment ili linkove u emalu.

5 Princip: Bezbednost računara zavisi od dva tipa zahteva: Funkcionalnih i uverenja

- Funkcionalni zahtevi
  - Opisuju šta bi sistem TREBAO DA RADI
- Uverenje (assurance)
  - Opisuju kako funkcionalni zahtevi trebaju da budu implementirani i testirani.
- Oba skupa zahteva su potrebni da se odgovori na sledeća pitanja:
  - Da li sistem radi prave stvari (kao što je propisano)?
  - Da li sistem radi prave stvari na pravi način?

5 Princip

- Ovo je slično ne IT oblastima kao što su verifikacija i validacija:
  - **Verifikacija** je proces potvrde da su ispunjene jedna ili više definisanih zahteva ili specifikacija.
  - **Validacija** određuje ispravnost ili kvalitet mehanizma koji se koristi da zadovolji potrebe.
- Primer sigurnost kola pojas za vezivanje:
  - Test verifikacije za pojas: test izdržljivosti na materijal, mehanizam brave,..
  - Validacija: provera pomoću testa sudara auta sa lutkama.
- Problem testiranje softvera se završava na validaciji

6 Princip: Zamagljivanje bezbednosti nije rešenje

- Mnogi ljudi smatraju da ukoliko hakeri ne znaju kako se softver štiti, bezbednost je bolja.
  - Iako ovo izgleda logično, nije tačno.
- Zamagliti bezbednost vodi do lažnog utiska bezbednosti, što može biti opasnije nego **ne** baviti se bezbednošću.
- Primer: open-source softver

7 Princip: Bezbednost = Upravljanje rizikom

- Bezbednost ne može da ukloni sve pretnje u sistemu ali može eliminisati većinu poznatih pretnji i minimizuje gubitak ako napadač uspe u iskorišćavanju slabosti.
- Trošenje više na bezbednost nego što je vrednost je besmisleno
- Procena i analiza rizika se koriste da dodaju ekonomsku vrednost “stvarima” da najbolje odrede odgovarajuće kontramere koje štite od gubitka.

7 Princip: Bezbednost: Upravljanje rizikom

- Dva faktora određuju rizik:
  - Koje su posledice gubitka?
  - Koja je verovatnoća da će doći do gubitka?

7 princip

Verovatnoća	Posledice (Značaj)				
	Nevažno	Malo	Srednje (moderate)	Značajno	Katastrofalno
A (skoro sigurno)					
B (verovatno)					
C (umereno)					
D (malo verovatno)					
E (retko)					

Matrica posledica/verovatnoće
1 Nizak, 2- Srednji, 3- Visok, 4- Ekstreman

7 princip

Verovatnoća	Posledice (Značaj)				
	Nevažno	Malo	Srednje	Značajno	Katastrofalno
A (skoro sigurno)	3	3	4	4	4
B (verovatno)	2	3	3	4	4
C (umereno)	1	2	3	4	4
D (malo verovatno)	1	1	2	3	4
E (retko)	1	1	2	3	3

Matrica posledica/verovatnoće
1 Nizak, 2- Srednji, 3- Visok, 4- Ekstreman

7Princip: Bezbednost=Upravljanje rizikom

- Ranjivost
  - Poznati problem u sistemu ili programu
- Exploit:
  - Program ili “cookbook” o tome kako da se iskoristi prednost specifične ranjivosti. Korišćenjem 'exploit'-a, napadač može neovlašćeno pristupiti ili koristiti aplikaciju ili operativni sistem.
- Napadač:
  - Link (veza) između ranjivosti i exploit-a

8 Princip: Tri tipa bezbednosne kontrole su preventivna, **otrkivajuća i odgovarajuća**

- Mehanizam bezbednosti služi za:
  - Prevenciju
  - Otkrivanje
  - Odgovor na napad dok se dešava ili nakon što je bio otkriven.

9 Princip: Kompleksnost je neprijatelj bezbednosti

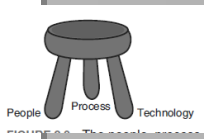
- Što je sistem kompleskiniji, teže ga je zaštiti.

10 Princip: Strah, nesigurnost i sumnja ne funkcionišu u “prodaji” bezbednosti.

- Menadžeri bezbednosti informacija moraju da opravdaju sva ulaganja i ona trebaju da budu zasnovana na dobrim, racionalnim poslovnim odlukama.
- Kada su potrebni resursi dobro obrazloženi, sa racionalnim poslovnim odlukama, zahtevi se retko odbijaju.

11 Princip: Ljudi, proces i tehnologija su svi potrebni da bi se zaštitio sistem

- Kontrola ljudi: dvostepena kontrola i odvajanje dužnosti
- Kontrola procesa se implementira da obezbedi da različiti ljudi mogu izvršavati istu operaciju na isti način svaki put
- Sama tehnologija bez ljudi i kontrole procesa nije uspešna
- Kontrole ljudi, procesa i tehnologije su esencijalni elementi bezbednosne prakse.



12 Princip: Otvoreno otkrivanje ranjivosti je dobro za bezbednost

- Skrivanje poznatih ranjivosti od korisnika i od programera može dovesti do lažnog osećaja bezbednosti.
- Potreba da znaju istinu omogućava korisnicima pravo da se zaštite.

Zaključak principi

- Neophodno je razumeti principe bezbednosti informacija
- Ovi principi su izmešani i napravljeni da opišu zašto određene bezbednosne funkcije i operacije postoje u realnom svetu ITa.

Literatura

- Kukrika, M. (2002). "Upravljanje sigurnošću informacija – zaštita informacionih sistema prema standardu ISO 17799", INFOhome Press, Beograd, 2002
- **D. Pleskonjić, N. Maček, B. Đorđević, M. Carić**, Mikro knjiga, Beograd, 2007., ISBN: 978-86-7555-305-2, knjiga – udžbenik.
- Merkow, M. & Breithaup, J. (2014) Information security: Principles and Practices, Pearson.

Dodatni izvori

- http://resources.infosecinstitute.com/guiding-principles-in-information-security/
- http://www.techrepublic.com/blog/it-security/the-**cia-triad**/