|  |
| --- |
| Fakultet tehničkih nauka Univerzitet u Novom Sadu |
| Secure deployment and disposal |
|  |
|  |
| **Tim 11** |
| **6/24/2020** |

|  |
| --- |
|  |

# System hardening

Većina računara ima za cilj da ograniči spoljni pristup sistemu. Softveri poput antivirusnih programa su namenjeni da spreče pokretanje zlonamernog softvera na mašini. I pored svega ovoga računari su još uvek podložni spoljnom pristupu. Ojačavanje sistema( *eng. System hardening)* je skup alata, tehnika i praksi koji služe da se ranjivosti u sistemu, aplikacijama i drugim oblastima svedu na minimum. Cilj ojačavanja sistema je da smanji rizik potencijalnih napada uklanjanjem suvišnih programa, aplikacija, portova, dozvola i tako dalje. Ojačavanje sistema je potrebno vršiti tokom čitavog životnog ciklusa, od početka instalacije, pa sve do održavanje i povlačenja iz produkcije.

Najčešće ranjivosti koje napadači iskoriste su:

* Lozinke i ostali akreditivi su smeštene u obične tekstualne datoteke
* Koriste se podrazumevanje lozinke (na primer 12345678)
* Loše konfigurisani BIOS, portovi, serveri ili drugi delovi infrastrukture
* Nedostatak privilegovanog pristupa

Nije najbolja praksa da se eliminisanje ranjivih delova sistema vrši u jednom koraku. Bolja opcija je da se napravi plan na osnovu pronađenih rizika koje sistem ima i da se prvo uklone oni koji predstavljaju najrizičniji deo. Potrebno je izvršiti detaljan pregled sistema u skladu sa tehnologijom koji podrazumeva penetraciono testiranje, skeniranje ranjivosti, upravljanje konfiguracijom i druge alate, koji omogućavaju pronalaženje nedostataka sistema. Preporuka je da se pridržavamo industrijskih standarda, kao što su NIST, Microsoft, CIS, DISA i drugi.

Prednosti ojačanog sistema je ta što je manji rizik od operativnih problema, pogrešnih konfiguracija i nekompatibilnosti. Smanjenjem površine napada sistem postaje manje rizičan, smanjena je mogućnost od kršenja podataka, neovlašćenih pristupa ili hakovanja sistema.

## Application Hardening

Ojačavanje aplikacije smanjujemo mogućnost da haker menja naš izvorni kod, omogućavamo da se aplikacija sigurno pokreće u svim okolnostima i vršimo zaštitu osetljivih podataka. Ako je aplikacija namenjena da se bavi finansijskim transakcijama, čuva lične podatke o korisniku ili sadrži podatke o nama ili nekom preduzeću jako je važno da je izvršimo ojačavanje aplikacije. Pre svega podrazumeva uklanjanje neiskorišćenih komponenti ili funkcija, ograničavanje pristupa aplikaciji na osnovu korisničkih uloga. Zatim se preporučuje izbegavanje ustaljenih lozinki, pored ovoga korisno je ograničiti minimalnu dužinu lozinke. Ojačavanje aplikacije vodi računa i o integrisanosti aplikacije sa drugim aplikacijama i uklanjanju suvišnih integracijskih komponenti i privilegija.

Metode ojačavanja aplikacije:

* Protection from Reverse Engineering:
* Code Obfuscation
* Anti-Debugging
* Binary Packing
* White-Box Cryptography
* Zaštita od neovlašćenog kršenja – postoji nekoliko načina da se spreči neovlašćena zloupotreba aplikacije neki od načina su:
  + Integrity Checking
  + Ios Jailbreak Detection
  + Android Rooting Detection

## Hardening OS

Ojačavanje operativnog sistema podrazumeva permisiju sistemskih komandi, loging svih aktivnosti, grešaka i upozorenja, kao i enkripciju lokalnog skladišta.

## Server Hardening

Ono što je najbitnije je da ojačavanje servera ima poente samo na onim serverima koji još uvek nisu povezani na internet. Ojačavanje servera se vrši kroz sigurnu konfiguraciju (*eng. security policy)*. Ključna stvar u sprečavanju najčešćih sajber-napade prema podacima CIS-a (*Center of Internet Security)* jeste da se pridržavamo propisanih primena za ojačavanje servera. Postoji više standardna u vezi sa ojačavanjem servera:

* SWIFT (*Society for Worldwide Interbank Financial Transactions) –* pruža sigurnosne kontrole u vezi sa finansijskim servisima.
* PCI DSS (*Payment Card Industrz Data Securitz Standard*) – primenjuju organizacije koje podržavaju onlajn plaćanje kreditnim karticama
* NIST (*National Institute of Standards and Technology*) – pruža skup standarda za potrebe informacionih sistema. Primer NIST-ovog standarda je NIST Cybersecuritz Framework koji obezbeđuje kategorizaciju podataka i informacija, koji se štite, razvoj bezbednih polisa, kao i procenu rizika i njihove efikasnosti.
* NERC-CIP (*North American Electric Reliabilitz Corp – Critical Infrastructure Protection*) – obuhvata standarde koji su u vezi sa električnim sistemima. Sastoji se od blizu 40 pravila.
* FFIEC (*Federal Financial Institution Examination Council*) – pruža regulative za finansijske institucije.

## Database Hardening

Poželjno je implementirati role-based access control, tako da bi samo korisnici sa posebnim privilegijama imali tu mogućnost da manipulišu nad podacima u bazi podataka. Podaci u bazi podataka bi trebalo da budu šifrovani, posebno podaci koji sadrže poverljive informacije. Trudite se da osoba koja ima pristup bazi podataka obavezno mora imati lozinku za pristup bazi podataka koja će biti komplikovana. Pored ovoga, potrebno je izbeći korišćenje baze podataka koja nema lozinku, pošto na taj način ona postaje dostupna svima.

## Network Hardening

Potrebno je osigurati tačke sistema, blokirati nekorišćene ili nepotrebne otvorene portove, kao i protokol i servise. Implementirati listu pristupa i enkriptovati sadržaj poruka koje se razmenjuju.

# Secure disposal procedure

Licencirani softverski programi, poslovni podaci, lični podaci se moraju pouzdano obrisati ili odložiti. Neuspeh u pravilnom brisanju predstavlja rizik, pošto se podaci mogu lako povratiti. Kada se datoteka obriše, operativni sistem ne uklanja datoteku u potpunosti sa diska. Brisanje datoteke uklanja samo referencu na datoteku iz tabele. Obrisana datoteka će ostati na disku dok se ne kreira nova datoteka preko originalne datoteke. Međutim, čak i tada je moguće izvršiti laboratorijski napad i oporaviti podatke iz originalne datoteke proučavanjem magnetnih polja.

Proces Secure Disposal uništava na nepovratan način osetljive informacije koje je koristio softver, koji se povlači iz produkcije. Potrebno je ispratiti propisan način uništavanja osetljivih podataka, kako se oni ne bi mogli vratiti.

Sanacija podataka podrazumeva uklanjanje klasifikacionih labela za date informacije i podatke. Metoda saniranja zavisi od informacija koje se čuvaju na medijumu, starosti medijuma i tako dalje. Zbog toga postoji nekoliko tehnika sanacije podataka:

* Clearing – prepisivanje adresibilnih lokacija medija random podacima uz pomoć hardverskih i softverskih rešenja. Potrebno je izdvojiti više prolaza, pored toga preporučuje se da se dodatno prepišu osetljivi podaci za brisanje. Postoje softveri koji realizuju ovaj način i dostupni su na Microsoft i Unix operativnim sistemima:
* Active@Kill Disk (Department of Defense Standard)
* DBAN Hard Drive Secure Wipe
* Windows Secure Eraser
* Secure Erase or Secure Empty Trash on Mac OS X 10.6.8 or later (3, 5, or 7 pass)
* Purging – konverzija podataka u nečitljivo stanje
* Destruction – Ako nije moguć primeniti neku od prethodnih opcija na kraju je potrebno fizički uništiti medijum na kom se nalaze podaci.

Secure Disposal regulative su ISO 27001 Controls i ISO 27002 Recommendations.

Prilikom skladištenja podataka potrebno je to vršiti u manjim količinama podataka i to iz više puta, kako velika količina nepotrebnih podataka prilikom skladištenja ne bi postala izvor osetljivih informacija, koje su potencijalno korisne napadačima. Pored ovoga, veoma je važno voditi računa o tome ko vrši skladištenje, odnosno obezbediti da se vrši beleženje ovih akcija u log fajl.