Secure deployment and disposal

System hardening

System hardening, ili jačanje sigurnosti sistema, jeste skup alata, tehnika i najboljih praksi za smanjenje ranjivosti u aplikacijama, sistemima, infrastrukturi, kao i drugim oblastima. Glavni cilj "učvršćivanja" sistema jeste poboljšanje ukupne IT bezbednosti i smanjenje rizika od napada na informacioni sistem. Kroz smanjenje rizika od curenja podataka, neovlašćenog pristupa i ubacivanja zlonamernog softvera, jačanje sigurnosti sistema igra ključnu ulogu u zaštiti osetljivih informacija i ozbezbedjivanju sigurnog računarskog okruženja.

Najbolje prakse učvršćivanja sistema:

- Revizija sistema
    - Vrši se koristeći alate za penetracijsko testiranje, skeniranje ranjivosti i upravljanje konfiguracijom. Potrebno je identifikovati nedostatke i prioritetizovati popravke koristeći industrijske standarde kao što su NIST, CIS, MICROSOFT i drugi.
- Strategija za jačanje sistema
    - Učvršćivanje sistema treba vršiti na osnovu rizika i prioriteta, odnosno fazno pristupiti i otkloniti najkritičnije nedostatke prvo.
- Brzo otkrivanje i "zakrpa" ranjivosti
    - Potrebno je omogućiti brzo i efikasno otkrivanje, kao i "zakrpu" ranjivosti, implementacijom automatizovanog sistema.
- Ažuriranje sistema
    - Redovno ažuriranje sistema podrazumeva primenu sigurnosnih patcheva softvera koje obezbeđuju proizvođači. Redovno ažuriranje sistema smanjuje rizik od iskorišćavanja poznatih sigurnosnih propusta.
- Ograničenje privilegije korisnika
    - Svaki korisnik treba da ima samo one privilegije koje su mu neophodne za izvršavanje svojih zadatka. Ovo se postiže kroz princip minimalnih privilegija čime se smanjuje rizik od zloupotrebe I neovlašćenog pristupa.
- Konfiguracija firewall-a
    - Firewall je zadužen za kontrolu pristupa mrežnog saobraćaji može se koristiti za blokiranje neovlašćenih ili sumnjivih konekcija. Osim toga, treba ograničiti mrežne servise i portove koji su otvoreni za komunikaciju kako bi se smanjila površina napada.
- Enkripcija podataka
    - Enkripcija se koristi za zaštitu osetljivih podataka tako da su oni nečitljivi za neovlašćene osobe. To se može postići enkripcijom u mirovanju (disk enkripcija) ili tokom prenosa podakata (TLS/SSL enkripcija).

- Bezbedno upravljanje lozinkama
    - Lozinke bi trebalo da budu složene, jedinstvene za svaki korisnički nalog i redovno se menjaju. Dodatno, korišćenje dvofaktorske autentifikacije pruža dodatni sloj sigurnosti pri prijavi na sistem.
    - Takođe, zaključavanje naloga nakon određenog broja neuspešnih prijava predstavlja dobru praksu.
- Sistemski logovi i monitoring
    - Sistemski logovi i monitoring su ključni za detekciju i reakciju na potencijalne sigurnosne incidente. Praćenje logova omogućava otkrivanje sumnjivih aktivnosti, upada ili zloupotreba. Analiza logova može pomoći u identifikovanju ranjivosti sistema i preduzimanju odgovarajućih koraka za njihovo otklanjanje.

Secure disposal najbolje prakse

Secure disposal predstavlja proces bezbedne i efikasne deinstalacije softverskih i hardverskih komponenti, uz istovremeno obezbeđivanje zaštite osetljivih podataka i umanjivanje potencijalnih bezbednosnih rizika. To je ključni aspekt upravljanja informacionom bezbednošću, budući da nepravilno odlaganje može dovesti do curenja podataka, neovlašćenog pristupa i pravnih posledica za organizacije. Da bismo osigurali sigurno odlaganje sistema, neophodno je slediti najbolje prakse koje obuhvataju tehničke i proceduralne mere.

- Inventar i klasifikacija podataka
    - Pre odlaganja sistema, organizacije treba da sprovedu detaljnu analizu podataka koji se čuvaju u njemu. Ova analiza pomaže u identifikaciji osetljivih ili poverljivih informacija koje zahtevaju posebno postupanje prilikom odlaganja. Podatke treba klasifikovati na osnovu njihove osetljivosti, regulatornih zahteva i eventualnih ugovornih obaveza kako bi se odredile odgovarajuće metode odlaganja.
- Sanitizacija podataka
    - Potpuno i nepovratno uklanjanje podataka sa medija za skladištenje je od ključne važnosti. Treba koristiti pouzdane metode koje se pridržavaju industrijskih standarda, kao što su prepisivanje podataka, degauziranje ili sigurno brisanje podataka pomoću sertifikovanih softverskih alata. Cilj je osigurati da ne mogu biti povraćeni nikakvi preostali podaci sa sistema.
- Uništavanje hardvera
    - Fizičko uništavanje hardverskih komponenti, poput hard diskova, često je neophodno kako bi se sprečilo eventualno vraćanje podataka.
- Bezbedno odlaganje
    - Osim brisanja podataka i uništavanja hardvera, važno je osigurati da sam proces odlaganja bude bezbedan. To podrazumeva odgovarajuće pakovanje i transport sistema, kako bi se sprečilo oštećenje ili gubitak podataka tokom transporta.
- Dokumentacija i revizija
    - Neophodno je voditi evidenciju o svim postupcima odlaganja sistema, uključujući inventar podataka, metode sanitizacije i uništavanja, kao i druge relevantne

informacije. Ova dokumentacija omogućava reviziju i proveru da su svi koraci sigurnog odlaganja bili sprovedeni ispravno.

Protokol za “Smart home” sistem

Postavljanje sistema u produkciju

Koraci:

- Planiranje i dizajn
    - Prvi korak u postavljanju pametne kuće u produkciju predstavlja detaljnu analizu objekata koje treba postaviti u sistem. Ovo uključuje pronalaženje kritičnih tačaka za bezbednost na objektima, kakvi uredjaji su nam potrebni za konkretan objekat i kako ih treba postaviti da bi se ispoštovale sve sigurnosne procedure i objekat bezbedno postavio u rad.
    - Nakon što se odredi potreban hardver, potrebno je odabrati pouzdan i siguran operativni sistem koji ce se instalirati na uredjaje. To najčešće predstavlja neku popularnu linux distribuciju.
    - Konačno, potrebno je odabrati server za infrastrukturu sistema, naš predlog je cloud platforma AWS kao industrijski standard za sigurnost, skalabilnost i visoku pouzdanost.
- Kupovina hardvera
    - Nakon što se napravi dizajn o svim potrebnim uredjajima za objekat, sledeći korak predstavlja kupovinu svih potrebnih uredjaja i senzora za funkcionisanje sistema.
- Instalacija sistema
    - Nakon što je sistem isplaniran i potrebni uredjaji kupljeni, potrebno je u objektu fizički instalirati sve uredjaje na odgovarajuća mesta kao sto je osmišljeno u dizajnu. Takodje im treba instalirati operativni sistem i povezati ih na internet, ukoliko svim uredjajima u kući internet nije dostupan potrebno je kupiti dodatnu mrežnu opremu.
- Povezivanje i konfiguracija
    - Nakon sto se uredjaji fizički instaliraju, treba ih konfigurisati i povezati kako bi se omogućila komunikacija izmedju uredjaja i smart home aplikacije. Ovo prvobitno predstavlja implementaciju sigurnosnih mera, postavljanje jakih lozinki, enkripciju podataka, instalaciju antivirusnih programa i ažuriranje softvera. Nakon konfigurisanja uredjaja potrebno je povezivanje sa aplikacijom tako što ćemo ih dodati u konfiguracioni fajl smart home aplikacije, definisati periode čitanja poruka, filtere u vidu regexa kao i uneti pravila za alarme specifične za ove uredjaje i objekat.
- Testiranje aplikacije i puštanje u rad
    - Nakon sto se sistem konfigurise i komponente povežu, treba sprovesti detaljno testiranje sistema, proveriti da li svi uredjaji funkcionišu kako bi

trebalo, da li se alarmi aktiviraju pravilno, kamere detektuju nepoznate objekte, senzori reaguju očekivano i slično.
    - Konačno, potrebno je testirati performanse sistema i ako je sve u redu staviti ga u rad.

- Obučavanje korisnika sistema
    - Potrebno je obučiti korisnike sistema Smart home za njegovu pravilnu upotrebu. Upoznati ih sa korisničkim interfejsom, dostupnim funkcionalnostima i kako se pravilno rukuje sa uredjajima. Takodje ih treba uputiti šta je potrebno raditi kada dodje do alarma i kritičnih situacija u objektu.

- Održavanje
    - Da bi sistem dugoročno funkcionisao bez problema, za korisnike smart home aplikacije treba obezbediti korisničku podršku, kao i redovne kontrole uredjaja koje bi sprovodili obučeni ljudi smart home tima.

Bezbedno uklanjanje sistema kada dođe do kraja njegovog životnog ciklusa

- Identifikacija osetljivih podataka
    - Prvi korak pri uklanjanju sistema je identifikacija osetljivih podataka. Osetljive podatke predstavljaju podaci koji bi mogli predstavljati rizik za organizaciju ili korisnike. U našem slucaju to predstavljaju informacije o vlasnicima i stanarima, konfiguracije njihovih objekata.

- Napraviti sigurnosnu kopiju podataka
    - Zatim je potrebno napraviti sigurnosnu kopiju osetljivih podataka identifikovanih u prethodnom koraku. Sačuvati je na sigurnom mestu. Ovim se obezbedjuje lakše postavljanje sistema u budućnosti ukoliko dodje do toga, što se dešava u praksi.

- Deinstalacija hardvera i brisanje podataka
    - Nakon pravljenja sigurnosne kopije osetljivih podataka može se preći na deinstaliranje uredjaja iz objekta. Uredjaje deinstalirati i obrisati podatke sa njih prateći propise proizvodjača zbog bezbednosti. Pojedine uredjaje kao što su hard diskovi, memorije (uredjaji za skladištenje) potrebno “uništiti” fizički ili specijalizovanim alatima za uništavanje podataka.

- Uklanjanje objekta iz sistema
    - Nakon uklanjanja hardvera, ukloniti objekat iz smart home aplikacije i sve podatke vezane za taj objekat, njegove uredjaje i slično.

- Dokumentacija i evidencija
    - Tokom celog procesa uklanjanja potrebno je voditi evidenciju o svim postupcima. Obezbediti potpisane potvrde o uklanjanju. Ovo će biti korisno za kasniju proveru da su svi koraci bili izvršeni u skladu sa bezbednosnim standardima i regulativama.