System hardening и secure disposal процедуре

System hardening је скуп алата, техника и пракси за редукцију рањивости. Заснива се на елиминисању потенцијалних делова система, који отварају врата нападачима. А то су непотребни програми, апликације, портови, пермисије, приступи итд. Постоји неколико типова system hardening-а: system hardening апликације, оперативног система, сервера, базе података и мреже.

Тип hardening-а , који треба подржати, зависи од ризика технологије, која се користи као и доступних ресурса. Неке од добрих пракси за приступ system hardening-у су:

- преглед постојећих система - детаљан преглед система у складу са технологијом подразумева пенетрационо тестирање (енг. penetration testing), скенирање рањивости (енг. vulnerability scanning), управаљње конфигурацијом (енг. configuration management) и друге алате, који омогућују проналажење недостатака система. При томе је пожељно служити се индустријским стандардима, као што су NIST, Microstoft, CIS, DISA и други.
- креирање стратегије systems hardening-а - није пожељно да се елиминација рањивих делова система врши у целости у једном кораку. Уместо тога, креира се план на основу пронађених ризика технологије коју систем обухвата, како би се најпре уклонили најризичнији делови.
- уклањање рањивости одмах након њихове идентификације - потребно је аутоматизовати, како идентификацију рањивости, тако и њихово решавање.
- hardening мреже - потребно је осигурати прописну конфигурацију firewall-а, осигурати тачке система, којима се приступа преко мреже, блокирати некоришћене или непотребне отворене портове, као и протоколе и сервисе. Имплементирати листе приступа и енкриптовати садржај порука, које се размењују.
- сервер hardening - hardening сервера никада не треба вршити над већ дистрибуираним серверима, односно онима који су повезани на интернет или неку екстерну мрежу. Избегавати инсталацију непотребног софтвера на сервер, прописно одвојити сервере система, осигурати функционалности суперкорисника и администратора додељивањем пермисија сервисима.
  - сервер hardening се врши кроз сигурну конфигурацију, тзв. "security policy" или "baseline". Прописна примена сервер hardening-а кључна је у сузбијању најчешћих сајбер-напада - према подацима CIS-а (Center of Internet Security), 85% покушаја крађе података може бити спречено применом 5 основних сигурносних корака, при чему сервер hardening заузима 3. место. Постоји више регулатива у вези са сервер hardening-ом:
    - PCI DSS (Payment Card Industry Data Security Standard) примењују организације, које подржавају онлајн плаћање кредитним картицама.
    - SWIFT (Society for Worldwide Interbank Financial Transactions) стандард пружа сигурносне контроле у вези са финансијским сервисима, који баратају подацима велике вредности. Под тиме се подразумева иницијализација, процесирање и одлагање финансијских трансакција.
    - NIST (National Institute of Standards and Technology) - америчка владина агенција за развој технологија, метрика и стандарда на пољу индустрије. Оно што је за нас релевантно, јесте то да NIST пружа скуп стандарда, односно, препорука сигурносних контрола за потребе информационих система. Пример широко распрострањеног NIST-овог

стандарда је NIST Cybersecurity Framework, који пружа категоризацију података и информација, који се штите, развој безбедносих полиса, као и процену ризика. Након имплементације безбедносих контрола, врши и процену њихове ефикасности.

- NERC-CIP - North American Electric Reliability Corp - Critical Infrastructure Protection. Обухвата стандарде, који су у вези са електричним системима. Састоји се од близу 40 правила и око 100 подзахтева. Садржи појмове "критичне компоненте" (Critical Assets) и "одговорни ентитети" (Responsible Entities). Критичне компоненте, између осталог, обухватају контролне системе, системе за добављање података, мрежну опрему, али и хардверске платформе виртуелних машина и виртуелна складишта.
- FFIEC (Federal Financial Insitutions Examination Council) - формално америчко владино тело, које пружа регулативе за финансијске институције.

- hardening апликације - подразумева уклањање свих непотребних компоненти или функција, затим, рестрикцију приступа апликацији базираној на корисничким улогама. Даље, избегавање дифолтних лозинки. Додатно, манипулација лозинки у оквиру апликације, требало би да буде под окриљем решења, која се воде најбољим праксама (password rotation, length итд.). Такође, hardening апликације бави се и инспекцијом интегрисаности апликације са другим апликацијама и системима, при чему се подразумева уклањање сувишних интеграцијских компоненти и привилегија.
- Hardening базе података - приступ бази података треба да буде привилегован - само корисници са посебним привилегијама могу да манипулишу над подацима базе. У ове сврхе, пожељно је имплементирати role-based access control; Подаци у бази треба да буду шифровани, а нарочито они, који носе поверљиве информације, као што су лозинке.
- Hardening оперативног система - обухвата енкрипцију локалног складишта (енг. local storage), пермисије системским командама, логинг свих активности, грешака и упозорења.
- Елиминација непотребних налога и привилегија .

У оквиру процеса Secure Disposal, осетљиве информације, којима је баратао софтвер, чији је прошао век трајања, неповратно се уништавају на сигуран начин. Неопходно је прибећи прописном уништавању оваквих података, јер, сада бескорисни подаци могу итекако бити корисни конкуренцији, која потенцијално може сазнати тајне и слабости датог система.

Пре него што се позабавим disposal регулативама, није на одмет напоменути начине санације података. Наиме, санација података подразумева уклањање класификационих лабела везаних за дате инфорамције и податке. Подаци могу бити смештени на неко од следећих медија: softcopy - у електронској репрезентацији и hardcopy - у физичкој репрезентацији. С тим у вези, постоји неколико техника санације података: Clearing - оверајдовање адресибилних локација медија рандом подацима, помоћу одговарајућих хардверских и софтверских решења; Purging - конверзија свих података у нечитљиво неповратно стање и, на крају, Destruction - уништавање самог медија на коме су подаци записани.

Secure Disposal регулативе су - ISO 27001 Controls и ISO 27002 Recommendations. Овим регулативама одређен је, између осталог, disposal медија:

- неке добре праксе су оверврајтовање, инсинерација, shredding итд.
- користити методе за лаку идентификацију медија, који захтевају disposal
- dispose медија миксовањем различитих типова, као што су CD, HDD, папир итд, како би се опоравак учинио тешким
- потребно је dispose вршити у мањим количинама података и то у више наврата, како велика количина непотребних података dispose-ована одједном, не би постала извор осетљивих инфомрација, које су потенцијално корисне нападачима.
- неопходно је повести рачуна о томе ко је извршио dispose, односно, потребно је обезбедити лог фајл, који ће забележити ову акцију.