Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti

Verzia dokumentu 2.1

Autor: CSIRT.SK

Dátum poslednej revízie: 19.10.2020 (v2.1)

Elektronická verzia originálu: https://www.csirt.gov.sk/informacna-bezpecnost/osvedcene-postupy/metodika-zabezpecenia-ikt-8a6.html

Podieľali sa

Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti (ďalej len *Metodika*) vznikla prepracovaním a rozšírením podkladov z dokumentu „Požiadavky na zabezpečenie infraštruktúry a riešenia implementovaného v rámci OPII“, ktorý vypracoval CSIRT.SK v spolupráci s ÚPVII SR (Úrad podpredsedu vlády SR pre investície a informatizáciu) v roku 2016.

Za podnety k obsahovej aj formálnej stránke ďakujeme kolegom z:

- Ministerstva Financií SR
- Združenia CZ-NIC
- Univerzity Pavla Jozefa Šafárika v Košiciach
- Univerzity Komenského v Bratislave
- a taktiež všetkým ďalším, ktorí sa na nás obrátili so spätnou väzbou.

Verzia a vývoj dokumentu

Vzhľadom na neustále sa vyvíjajúce a meniace techniky útokov a obrany je táto metodika žijúcim dokumentom. K metodike sú priebežne zhromažďované podnety na doplnenie a zmeny podľa aktuálneho vývoja. Tieto zmeny budú občasne zakomponované do novej verzie metodiky, ktorá bude zverejnená na webstránkach https://www.csirt.gov.sk.

Akékoľvek podnety k vylepšeniu obsahu metodiky prosím posielajte na *info@csirt.sk.*

Obsah

Úvod

Informačné systémy a prostriedky používané v organizácií musia byť zabezpečené takým spôsobom, aby sťažovali kompromitáciu infraštruktúry a aby v prípade kompromitácie služby alebo systému boli dôsledky incidentu minimalizované. To znamená, že ak útočník kompromituje časť infraštruktúry, je pre neho zložité dostať sa ďalej a kompromitovať ďalšiu časť infraštruktúry – to znamená je obmedzená možnosť pivotingu. Je nutné implementovať viacúrovňovú hĺbkovú ochranu.

Cieľ dokumentu

Tento dokument sumarizuje minimálne opatrenia potrebné na zabezpečenie informačných systémov a infraštruktúry organizácie tak aby platili princípy uvedené v úvode.

Metodika je cielená pre využitie vo verejnej správe pre organizácie so zvýšenými požiadavkami na bezpečnosť[1], avšak v princípe je aplikovateľná pre akékoľvek veľké alebo stredne veľké počítačové siete, ktoré majú zvýšené požiadavky na bezpečnosť, ale potrebuju mať zabezpečenú kybernetickú bezpečnosť na úrovni odolnosti voči štandardným cieleným kybernetickým útokom.

V dokumente sa používajú kľúčové slová „musí“, „malo by byť“, „odporúča sa“. Tieto sú ohodnotením dôležitosti daného opatrenia s ohľadom na jeho implementačnú náročnosť. Ak sa organizácia rozhodne byť v súlade s metodikou, platí pre ne význam podľa vysvetlenia v kapitole „Definícia významu kľúčových slov“.

Dokument neobsahuje podrobné implementačné detaily jednotlivých opatrení. Podrobné implementačné detaily budú uvádzané v jednotlivých dokumentoch postupne zverejňovaných na stránkach špecializovaného útvaru CSIRT.SK.

Aj v prípade, že dokument nebude implementovaný ako celok, jednotlivé (najmä technické) opatrenia boli vybrané tak, aby pokrývali jeden alebo viacero vektorov útoku. V prípade správnej implementácie konkrétneho opatrenia bude infraštruktúra organizácie odolná alebo v niektorých prípadoch až imúnna voči útokom zneužívajúcim zraniteľnosť opravovanú daným opatrením.

Komu je dokument určený

Dokument je určený primárne pre organizácie verejnej správy so zvýšenými požiadavkami na bezpečnosť. Čerpať z neho však môžu aj ďalšie organizácie a inštitúcie z rôznych sektorov, od súkromného cez verejný až po akademickú obec. Podľa toho, akú úroveň riadenia informačnej bezpečnosti organizácia implementujúca opatrenia podľa tejto metodiky už má, možno zvoliť, kto bude zavedenie odporúčaní garantovať.

1 Napríklad v zmysle Metodiky prevencie a pripravenosti (ktorá bola vypracovaná špecializovaným útvarom CSIRT.SK v zmysle úlohy 3.1. Akčného plánu ku Koncepcií kybernetickej bezpečnosti schválenej vládou SR na roky 2015-2020).

V prípade, že organizácia má vybudovanú istú štruktúru riadenia informačnej bezpečnosti, môže zodpovednosť za zavedenie metodiky do praxe prebrať manažér bezpečnosti alebo ním poverená osoba/osoby. Ak však inštitúcia nemá vybudované takéto kapacity, môže použiť metodiku v začiatkoch ich budovania. Zavedenie organizačných opatrení bude v kompetencii vedenia inštitúcie. Inštitúcia môže čerpať informácie o organizačnej bezpečnosti aj z iných zdrojov, napr. norma ISO 27002. Podobné dokumenty však bývajú rozsiahle, preto sa metodike sumarizujú základné body, ktoré sú pre zavedenie organizačnej bezpečnosti kľúčové.

Aj v prípade, že organizácia nemá kapacity na vytvorenie hierarchie manažmentu informačnej bezpečnosti (IB), môžu technické odporúčania metodiky použiť samotní administrátori informačných systémov, v medziach svojich kompetencií pri spravovaní predmetných zabezpečovaných IS.

Rozsah a záber dokumentu

Tento dokument špecifikuje opatrenia na zabezpečenie IS nasadzovaných do infraštruktúr organizácie verejnej správy.

Bezpečnostné opatrenia sa delia do týchto skupín:

1. Organizačné opatrenia – organizačné zabezpečenie bezpečnosti IS
2. Technické opatrenia – technické zabezpečenie bezpečnosti IS
3. Administratívne opatrenia – súhrn smerníc, politík a pracovných postupov, ktoré musia byť implementované na zabezpečenie základnej úrovne bezpečnosti IS v závislosti od jeho typu

Obmedzenia

Dokument sa v tejto verzií nezaoberá špecifickými požiadavkami na: fyzickú bezpečnosť infraštruktúry, bezpečnosť mobilných zariadení, bezpečnosť Internetu vecí (IoT – Internet of Things), bezpečnosť ICS systémov (Industrial Control Systems), zabezpečenie služieb využívajúcich IPv4 multicast, zabezpečenie webových služieb (web services).

Definícia významu kľúčových slov

V tomto dokumente sú použité nasledujúce kľúčové slová podľa uvedeného významu:

„musí“ – špecifikuje povinnú požiadavku (platí aj pre „je nutné“)

„nesmie“ – špecifikuje povinný zákaz

***„malo by* [byť]”** – špecifikuje požiadavku, ktorá je povinná pokiaľ neexistuje pádny dôvod prečo nemôže byť splnená. Ak existuje takýto dôvod, musí byť zdokumentovaný a schválený.

“*nemalo by* [byť]” - špecifikuje zákaz, ktorý je povinný pokiaľ neexistuje pádny dôvod prečo nie je možné ho splniť. Ak existuje takýto dôvod, musí byť zdokumentovaný a schválený.

“*odporúča sa*” – špecifikuje odporúčanú požiadavku (platí aj pre “je vhodné”)

Ak je rozdiel medzi operátorom (musí / malo by byť / odporúča sa) v konkrétnom opatrení a jeho nadradeným číslovaných bodom, tak platí operátor v konkrétnej odrážke (to znamená posledný špecifikovaný). *V nasledujúcom príklade pre bod b) platí operátor „malo by byť“:*

1.1 V organizácii musí byť vykonávané pravidelné monitorovanie a preskúmavanie bezpečnosti IS v rozsahu:

a. Pravidelné preskúmavanie plnenia cieľov bezpečnostnej politiky aspoň raz za 12 mesiacov vedením organizácie.

b. Malo by byť vykonávané pravidelné testovanie záloh dôležitých systémov na kontrolu funkčnosti.

Vysvetlenie skratiek

ACL - Access Control List

AP - Access Point

CSRF - Cross-Site Request Forgery

DHCP - Dynamic Host Configuration Protocol

DMZ - Demilitarized Zone - VLAN, v ktorej sú umiestnené servery poskytujúce služby do externej siete, ktorá je logicky oddelená od inernej siete (komunikácia je fultrovaná sieťovým firewallom)

DNS - Domain Name System

DoS – Denial of Service

FW – Firewall

IB – Informačná bezpečnosť

ICS - Industrial Control System

MitM útok – Man in the Middle útok

MVC – návrhový vzor Model–View–Controller

MVP - návrhový vzor Model–View–Presenter

NAC – Network Access Control

NAP - Network Access Protection

NDP - Neighbor Discovery Protocol - protokol v IPv6, okrem iného, nahradzujúci ARP z IPv4

NTP - Network Time Protocol

OS - Operačný systém

PVLAN – Private VLAN

princíp least privilege

RDP - Remote Desktop Protocol

QoS - Quality of Service

Sieťový firewall - firewall umiestnený v sieti filtrujúci komunikáciu viacerých zariadení, prípadne sietí (nie lokálny firewall)

SNMP – Simple Network Management Protocol

SSO – Single Sign-On

Telepresence

UAC – User Access Control

VLAN – Virtual Local Area Network

VPN – Virtual Private Network

VOIP – Voice over IP

WAF – Webaplikačný firewall - špeciálny typ firewallu, prispôsobený na zabezpečenie webového servera. Ide o filter, plugin či zariadenie ktorý aplikuje set pravidiel na HTTP prevádzku.

Whitelisting - metóda kontroly prístupu k službám, ktorá povoľuje prístup iba špecifikovaným klientom a všetkým ostatným ho zakazuje

XSS - Cross-Site Scripting

Bezpečnostné požiadavky

Požiadavky na bezpečnostné opatrenia na zaistenie bezpečnosti infraštruktúry a implementovaného riešenia sa delia na:

1. Organizačné opatrenia
2. Technické opatrenia
    a. zabezpečenie implementovaného riešenia
    b. zabezpečenie služieb dostupných z externých sietí – Webové aplikácie
    c. zabezpečenie infraštruktúry
    d. zabezpečenie externej infraštruktúry
    e. zabezpečenie internej infraštruktúry
    f. zabezpečenie pracovných staníc pristupujúcich k implementovanému riešeniu
3. Administratívne opatrenia

1. Organizačné opatrenia

Všeobecné požiadavky

1.2 V organizácii musia byť zavedené aspoň nasledovné opatrenia personálnej bezpečnosti:

c. Sú určené roly a zodpovednosti za informačnú bezpečnosť aspoň pre tieto roly: vrcholný predstaviteľ organizácie, manažér pre bezpečnosť, vedúci pracovník, administrátor, audítor, používateľ.
d. Roly manažéra pre bezpečnosť a audítora musia byť oddelené od oddelenia správy IKT.
e. Pred prijatím do pracovného pomeru je vykonávané preverenie osôb (aspoň poskytnutím výpisu z registra trestov).
f. Zodpovednosť za informačnú bezpečnosť je zahrnutá do pracovných zmlúv so zamestnancami spolu so sankciami v prípade nedodržania týchto povinností.
g. So zamestnancami a tretími stranami (napríklad dodávateľmi) sú podpísané dohody o mlčanlivosti.
h. V prípade ukončenia pracovného pomeru sú zamestnancovi včas odobraté prístupové práva, všetky zverené aktíva a informácie sú včas navrátené a všetky zdieľané heslá sú zmenené.

1.3 V organizácii musí byť zavedené riadenie informačných aktív s nasledovnými požiadavkami:

a. Organizácia musí mať vypracovaný inventár informačných aktív, ktorý je úplný, aktuálny, preskúmavaný a aktualizovaný pri zmenách v IS, minimálne však každých 12 mesiacov.
b. Na vedenie, údržbu a aktualizáciu inventáru aktív by mala byť stanovená zodpovedná osoba.
c. Každé aktívum musí mať prideleného vlastníka, ktorý zodpovedá za jeho bezpečnosť.
d. V organizácii musí byť implementovaný mechanizmus klasifikácie informácií z hľadiska dôvernosti.
e. Informácie musia byť označované príslušným klasifikačným stupňom.
f. Pre každý klasifikačný stupeň musí byť definovaný súbor opatrení, ktoré popisujú požiadavky na ich ochranu pri ukladaní, prenose a spracúvaní.
g. Inštalácia softvéru a hardvéru musí byť vykonávaná len povereným administrátorom.
h. V organizácii musí byť vypracovaný zoznam autorizovaného softvéru a je dovolené inštalovať výhradne legálny softvér z tohto zoznamu získaný z dôveryhodných zdrojov .
i. V organizácii by mal byť vypracovaný zoznam autorizovaného hardvéru na základe sériového čísla a je dovolené používať výhradne hardvér z tohto zoznamu, pričom výnimky musia byť schválené manažérom bezpečnosti.
j. V organizácii musí byť vypracovaná a pri zmenách aktualizovaná dokumentácia o sieťovej topológii a technická dokumentácia o IS.
k. Nepotrebné informácie a ich dátové nosiče musia byť mazané a ničené bezpečným spôsobom.
l. V organizácii by mal byť implementovaný systém pre riadenie zmien.
m. V organizácii by mal byť implementovaný systém pre riadenie záplat.

1.4 V organizácii musí byť implementovaný systém manažmentu rizík, ktorý spĺňa aspoň nasledovné požiadavky:

a. Identifikácia a ohodnotenie rizík je založené na identifikácii a ohodnotení aktív, ich zraniteľností a hrozieb, ktoré majú potenciál tieto zraniteľnosti zneužiť, a potenciálnych dopadov pri zneužití zraniteľností.
b. Identifikácia a ohodnotenie rizík je vykonávané konzistentným, systematickým, vopred stanoveným a dokumentovaným spôsobom, ktorý zaručí pokrytie všetkých známych rizík a opakovateľnosť výsledkov.
c. Je stanovená a vedením schválená miera akceptovateľných rizík a všetky riziká s vyššou hodnotou ako je miera akceptovateľných rizík sú ošetrené tak, aby zvyškové riziko nepresiahlo mieru akceptovateľných rizík.
d. Je stanovené, čo organizácia pre adekvátne ošetrenie rizika vyžaduje: môže ísť o jeho okamžité odstránenie, resp. je stanovená lehota, počas ktorej môže byť riziko prítomne, nakoľko ešte nie je dostupné riešenie (napríklad vydanie záplaty dodávateľom IS, v ktorom sa objavila nová kritická zraniteľnosť).
e. Je vedený zoznam zostatkových rizík a tieto riziká sú v pravidelných intervaloch a pri zmenách v IS a prostredí organizácie preskúmavané.
f. Riziká sú ošetrované podľa Plánu pre ošetrovanie rizík so stanovenými konkrétnymi opatreniami, zodpovednosťami za implementáciu týchto opatrení, termínmi a potrebnými zdrojmi na ošetrenie rizík.

1.5 V organizácii musia byť stanovené a dodržiavané aspoň nasledovné pravidlá pre používateľov IS:

a. Pri odchode od pracovnej stanice je zamestnanec povinný ju uzamknúť.
b. Pri zadávaní hesla musí zamestnanec dbať na to, aby nebolo náhodne odpozorované.
c. Heslá musia byť rôzne pre rôzne IS s výnimkou SSO (Single Sign-On).
d. Heslá by nemali byť zdieľané.
e. Heslá nesmú byť voľne dostupné prostredníctvom fyzických alebo dátových prostriedkov.
f. Pri prenášaní informácií a príloh citlivých z hľadiska dôvernosti prostredníctvom e-mailu sa musí používať šifrovanie.
g. Pri prenášaní informácií a príloh citlivých z hľadiska integrity alebo autentickosti prostredníctvom e-mailu sa musí používať podpisovanie.

1.6 V organizácii by mali byť stanovené a dodržiavané aspoň nasledovné pravidlá pre používateľov IS:

a. Je zakázané používať súkromné prostriedky na služobné účely.
b. Je zakázané používať služobné prostriedky na súkromné účely.
c. Pri práci s e-mailom je zakázané otvárať nevyžiadanú poštu, ako aj prílohy e-mailov a odkazy obsiahnuté v tele e-mailov z nedôveryhodných zdrojov.
d. Je zakázané pristupovať k webovým portálom, ktoré môžu ohroziť bezpečnosť pracovnej stanice (známe škodlivé webové stránky, pornografické stránky, stránky poskytujúce

akúkoľvek formu sťahovania pirátskeho obsahu, stránky poskytujúce akúkoľvek formu hazardu, stránky o hackingu a podobne)

e. Je zakázané pristupovať k sociálnym sieťam a chatovacím programom s výnimkou sociálnych sietí a chatovacích programov používaných pre pracovné účely.
f. Pre prácu s Internetom je povolené používať len zabezpečený prehliadač s nainštalovanými a vhodne nakonfigurovanými bezpečnostnými doplnkami blokujúcimi JavaScript, reklamy a Adobe Flash. V odôvodnených prípadoch pokiaľ bezpečnostné doplnky bránia vo výkone pracovných povinnosti, je možné pre dôveryhodné webové stránky udeliť dočasnú výnimku pre konkrétnu doménu. Upozorňujeme, že je potrebné zaškoliť používateľov ako používať tieto doplnky.

1.7 V organizácii musia byť stanovené a dodržiavané aspoň nasledovné pravidlá pre administrátorov IS:

a. V prípade odchodu a po ukončení práce so stanicou (resp. konzolou alebo terminálom) je potrebné sa odhlásiť.
b. Heslá k privilegovaným a administrátorským účtom musia spĺňať požiadavky uvedené v Prílohe A.
c. Je zakázané zaznamenávať a zasielať heslá v otvorenom a reverzibilnom tvare.
d. Zdieľanie hesiel by malo byť zakázané[2].
e. Akékoľvek zmeny v systémovej konfigurácii sú dokumentované.
f. Používateľom je možné poskytnúť len prístup v minimálnom rozsahu nevyhnutnom na vykonávanie ich pracovných činností.
g. Pri ukončení pracovného pomeru s administrátorom musí byť zablokované jeho konto na autentifikačnom serveri ako aj na zariadeniach, ktoré boli pod jeho správou a odporúča sa vykonať zmeny jemu známych autentifikačných údajov (príklad: SNMP community strings, failover kľúče, kľúče smerovacích protokolov, VPN kľúče).
h. Pri ukončení pracovného pomeru s administrátorom je nutné zablokovať jeho účet na prístup cez VPN a zmeniť akékoľvek zdieľané správcovské prístupové údaje.
i. Pri ukončení pracovného pomeru s administrátorom by mala byť skontrolovaná integrita konfigurácií všetkých prvkov (napr. konfigurácia SNMP, Syslog), konfigurácia správcovských prístupových údajov a konfigurácia správcovských prístupových metód.

1.8 V organizácii musí byť zavedené riadenie fyzického a logického prístupu s nasledovnými pravidlami:

a. Prideľovanie oprávnení sa vykonáva v nasledovných krokoch: návrh, schválenie a nastavenie prístupových oprávnení.
b. Prístupy sú prideľované len v rozsahu nevyhnutnom na vykonávanie pracovných činností.
c. Je vypracovaný a aktualizovaný zoznam privilegovaných prístupových oprávnení a pravidelný ročný audit ich potreby.

2 V prípade, že je zdieľanie hesiel nutné (napr. administrátorské a servisné účty), musia byť bezpečne skladované prostredníctvom šifrovaných zdieľaných úložísk. Zdieľanie hesiel musí byť odôvodnené a dokumentované, musí byť stanovené, kto má k zdieľaným heslám prístup a takýchto hesiel musí byť minimum

d. Všetky heslá k privilegovaným prístupovým účtom musia spĺňať kritériá pre administrátorské účty uvedené v Prílohe A.

1.9 V organizácii musia byť zavedené a dodržiavané postupy pre zálohovanie v rozsahu:

a. Frekvencia a rozsah zálohovania musí byť schválená vedením organizácie a musí byť dokumentovaná.
b. Zamestnanci zodpovední za zálohovanie sú určení a sú poučení o svojich povinnostiach.
c. Musí byť stanovený interval, čas, rozsah dát, dátové médium a vedenie dokumentácie o zálohovaní.
d. Zálohy musia byť umiestnené v zabezpečenom priestore s riadením vstupu.
e. Zálohy kritických informácií a IS musia byť uložené aj na fyzicky dostatočne vzdialenej lokalite a musia byť šifrované.
f. Musí byť pravidelne vykonávaný test obnovy záloh.

1.10 V organizácii musí byť zavedený systém riadenia kontinuity činností s nasledovnými požiadavkami:

a. V organizácii musia byť stanovené roly a zodpovednosti pre plnenie havarijných plánov a plánov obnovy.
b. V organizácii musí byť stanovená cieľová doba obnovy (RTO) a cieľový bod obnovy (RPO) pre jednotlivé procesy, IS a aplikácie.
c. Jednotlivé postupy pri riadení kontinuity činností by mali byť pravidelne testované prostredníctvom ohlásených alebo neohlásených cvičení.

1.11 V organizácii musia byť zavedené a dodržiavané postupy pre nahlasovanie a riešenie počítačových bezpečnostných incidentov aspoň v rozsahu:

a. Je stanovené kontaktné miesto pre nahlasovanie incidentov a roly a zodpovednosti pre zamestnancov poverených ich riešením.
b. Kontaktné údaje pre nahlasovanie počítačových incidentov sú nahlásené špecializovanému útvaru pre riešenie počítačových incidentov CSIRT.SK a pri zmenách kontaktných údajov sú nové kontaktné údaje opätovne nahlásené.
c. Je vedená a udržiavaná evidencia kontaktných údajov tretích strán potrebných na riešenie počítačových incidentov a je určená osoba zodpovedná za jej vedenie a udržiavanie.
d. Zamestnanci poverení riešením incidentov sú odborne spôsobilí, pravidelne školení a zastupiteľní.
e. Incidenty sú klasifikované podľa klasifikačnej schémy definovanej v smernici pre riešenie počítačových incidentov.
f. Na detekciu a riešenie incidentov sú vyhradené dostatočné zdroje (finančné, ľudské...).
g. Incidenty sú riešené bez zbytočného odkladu podľa vopred stanovených postupov.
h. Sú vytvorené eskalačné postupy.
i. Je vedená evidencia bezpečnostných incidentov a je určená osoba zodpovedná za jej vedenie.
j. Po vyriešení incidentu je vykonaná následná analýza a sú implementované opatrenia na predchádzanie incidentom podobného typu.

k. Po vyriešení incidentu je vykonané preskúmanie postupu jeho riešenia, sú identifikované nedostatky a návrhy na zlepšenie (napr. vhodnosť alebo potreba nových nástrojov, dostatok personálu, potreba školení a podobne), tieto sú prediskutované na stretnutí zamestnancov riešiacich bezpečnosť v organizácii a závery z tohto stretnutia sú dokumentované.
l. Sú vytvorené plány pre riešenie počítačových incidentov aspoň tohto typu: prienik, nákaza škodlivým kódom, DoS útok, sociálne inžinierstvo (phishing, impersonácia a pod) Odporúča sa implementovať postupy pre riešenie incidentov – napríklad postupy zverejnené národnou, vládnou alebo rezortnou jednotkou CSIRT / CERT.

1.12 V organizácii musí byť zavedené kontinuálne zvyšovanie povedomia o informačnej bezpečnosti, súvisiacich hrozbách a možnostiach ochrany pred týmito hrozbami aspoň v rozsahu:
a. Existujúci vedením schválený program vzdelávania s určenou zodpovednosťou za jeho plnenie a vyhradenými zdrojmi.
b. Vzdelávací proces je pravidelný, vyhodnocovaný a neustále zlepšovaný. Odporúča sa, aby boli súčasťou overenia efektivity vzdelávacieho procesu používateľov aj neohlásené testy (napríklad prostredníctvom sociálneho inžinierstva a vedomostných testov).
c. Zvyšovanie povedomia zahŕňa predstavenie typov informácií, ich klasifikáciu a označovanie, predstavenie súčasných hrozieb a spôsobov ochrany voči nim, poučenie o postupoch pre identifikáciu a nahlasovanie bezpečnostných incidentov a určenie kontaktného miesta pre ich nahlásenie.

1.13 Organizácia musí vykonávať audity bezpečnosti IS aspoň raz za 36 mesiacov podľa nasledovných požiadaviek:
a. Je vypracovaný program auditov na obdobie troch rokov, ktorý zahŕňa interné audity, posúdenie zraniteľností a penetračné testy.
b. Pre každý interný audit je vypracovaný plán auditu, ktorý obsahuje ciele auditu, referenčné dokumenty, dátumy a miesta vykonania auditu, organizačné útvary, ktoré sú predmetom auditu, roly a zodpovednosti.
c. Audítor musí byť nezávislý[3], skúsený, musí byť znalý príslušnej legislatívy a štandardov a musí mať vhodné osobnostné predpoklady.
d. Správa z auditu musí obsahovať aspoň zoznam účastníkov auditu, zoznam zistených nezhôd, pozorovaní a príležitostí na zlepšenie, vyjadrenie audítora k rozsahu v akom organizácia plní bezpečnostné požiadavky a návrh opatrení.
e. Pre implementáciu opatrení na odstránenie zistených nedostatkov je potrebné vypracovať plán implementácie opatrení podľa ich priority s určením zodpovedností, termínov plnenia a zdrojov.

3 Funkcia audítora musí byť organizačne nezávislá od oblasti alebo činnosti, ktorá je predmetom auditu tak, aby umožnila jeho objektívne vykonanie a zamedzila takým vplyvom na audítora, ktoré by mohli ohroziť jeho integritu, objektivitu, profesionálny skepticizmus a úsudok.

1.14 Prístup tretích strán ako aj ich vzdialený prístup musí byť riadený, kontrolovaný a prístupové oprávnenia musia byť udelené len v minimálnom rozsahu potrebnom na vykonávanie pracovných činností.

1.15 Tretie strany musia organizácii na požiadanie poskytnúť správu o stave zabezpečenia a funkčnosti zverených aktív v rozsahu stanovenom organizáciou na základe povahy predmetných aktív.

1.16 Pre kritické systémy by malo byť implementované monitorovanie dostupnosti služieb a detekcia anomálií.

1.17 Pred nasadením IPv6 do prevádzky musí byť vytvorený plán nasadenia, ktorý obsahuje aj analýzu rizík spojených s IPv6 a požiadavky na bezpečnostné mechanizmy a konfiguráciu infraštruktúry.

1.18 Ak sa používa IPv6, musí byť zabezpečené, že sieťoví administrátori, operátori monitoringu aj bezpečnostný tím majú dostatočné technické znalosti špecifík IPv6 protokolu aj podporných protokolov ako ICMPv6, DHCPv6, DNS.

1.19 Pred nasadením VOIP alebo telepresence musí byť vytvorený plán nasadenia, ktorý obsahuje aj analýzu rizík spojených s VOIP a telepresence a požiadavky na bezpečnostné mechanizmy a konfiguráciu infraštruktúry.

Mechanizmus kontroly

1.20 V organizácii musí byť vykonávané pravidelné monitorovanie a preskúmavanie bezpečnosti IS v rozsahu:

a. Pravidelné preskúmavanie plnenia cieľov bezpečnostnej politiky aspoň raz za 12 mesiacov vedením organizácie.
b. Kontinuálne monitorovanie účinnosti bezpečnostných opatrení na ošetrenie rizík.
c. Pravidelné preskúmavanie zostatkových rizík aspoň raz za 12 mesiacov a v prípade zmien v IS.
d. Pravidelné monitorovanie log záznamov a ich analýza aspoň raz za týždeň.
e. Pravidelná kontrola technického stavu zariadení a funkčnosti aplikácií aspoň raz za mesiac.
f. Pre kritické systémy musí byť vykonávané monitorovanie funkčnosti aplikácií v reálnom čase.
g. Malo by byť vykonávané pravidelné testovanie záloh dôležitých systémov na kontrolu funkčnosti.
h. Je vykonávaná pravidelná kontrola prístupových oprávnení a deaktivovanie nepotrebných prístupových účtov aspoň každých 12 mesiacov.
i. Pravidelné meranie účinnosti programu vzdelávania zamestnancov a testovanie úrovne ich bezpečnostného povedomia.
j. Pravidelné preskúmavanie jednotlivých stratégií a plánov pre kontinuitu činností aspoň raz za 12 mesiacov.

1.21 Každých 24 mesiacov by malo byť vykonávané interné a externé penetračné testovanie IS organizácie. V prípade, že posledný penetračný test znamenal kompromitáciu dôležitého systému alebo kompromitáciu značnej časti infraštruktúry, mal by byť vykonať ďalší penetračný test hneď po odstránení zraniteľností – najneskôr však o 12 mesiacov.

Technické opatrenia

2 Minimálne požiadavky na zabezpečenie implementovaného riešenia

Bezpečnosť životného cyklu IS

Pri vývoji riešenia je potrebné myslieť na bezpečnosť už od začiatku a prispôsobiť tomu návrh aj implementáciu samotného riešenia počas jednotlivých fáz.

Návrh riešenia

2.1 Navrhnuté riešenie musí mať modulárnu štruktúru, pričom
   a. Pri návrhu jednotlivých komponentov riešenia musí byť splnený princíp least privilege a všetky entity (t.j. používatelia aj systémy) musia mať prístup iba k údajom / aktívam, ktoré pre svoju činnosť nevyhnutne potrebujú.
   b. Architektúra riešenia by mala byť trojvrstvová – mala by pozostávať z prezentačných serverov, aplikačných serverov a databázových serverov,
   c. Odporúčané je použitie overených návrhových vzorov, napr. MVC, resp. MVP

2.2 Musia byť identifikované všetky súčasti (interné aj externé[4]), od ktorých závisí riešenie. Pre jednotlivé súčasti musia byť identifikované zraniteľnosti, ktoré sa v nich môžu vyskytnúť a vyhodnotiť riziká zneužitia týchto zraniteľností na základe:
   a. prístupového vektoru útočníka (lokálny prístup/sieť),
   b. náročnosti získania prístupu,
   c. potreby autentifikácie,
   d. dopadov úspešného útoku na dostupnosť, integritu a dôvernosť riešenia a údajov v ňom spracovávaných.

2.3 Na základe analýzy rizík musia byť navrhnuté opatrenia, ako predchádzať možným incidentom a ako postupovať v prípade vzniku incidentu. Tieto opatrenia musia byť zapracované v návrhu riešenia.

Implementácia riešenia

2.4 Riešenie musí byť vyvíjané v bezpečnom vývojovom prostredí.

2.5 Pri implementácii by mali byť použité dôveryhodné (a zároveň široko rozšírené) frameworky / knižnice, ktoré kladú dôraz na bezpečnosť a predchádzanie bežným programátorským chybám a zároveň často a rýchlo zverejňujú opravy bezpečnostných chýb.

2.6 V prípade, že implementované riešenie potrebuje spracovávať dôverné údaje (napr. osobné údaje), počas vývoja aj testovania musia byť použité anonymizované, resp. fiktívne údaje.

4 Napr. knižnice a komponenty dodané tretími stranami; systémy, na ktorých bude riešenie postavené alebo ktoré bude využívať pri svojej prevádzke

2.7 Pri písaní zdrojového kódu by mal byť použitý systém na verzionovanie[5], pričom:
   a. jednotlivé zmeny (commity) by mali byť digitálne podpísané privátnym kľúčom autora daného commitu,
   b. commity by mali mať zmysluplné popisy,
   c. mala by byť implementovaná automatická kontrola zdrojového kódu na prítomnosť chýb a testovanie po každom commite.

2.8 Nemali by byť použité funkcie/volania/nástroje, ktoré sú podľa ich dokumentácie v súčasnej dobe zastarané (angl. deprecated) alebo nebezpečné (angl. unsafe) a mali by byť nahradené odporúčanými alternatívami.

2.9 Počas vývoja riešenia musia byť povolené všetky bezpečnostné vlastnosti použitých nástrojov, najmä však:
   a. zapnuté všetky varovania a ochrany vývojových nástrojov[6]
   b. varovania vývojového prostredia

2.10 Všetky varovania z predchádzajúceho bodu by mali byť opravené.

2.11 Počas vývoja musí byť vedená vývojárska dokumentácia:
   a. dokumentácia musí obsahovať bližší popis kľúčových častí riešenia až na prípadné výnimky chránené obchodným tajomstvom; tieto výnimky však musia byť zaznamenané v dokumentácii
   b. v dokumentácii musí byť zaznamenaná každá zmena oproti pôvodnej špecifikácií a jej dôvody a každá takáto zmena musí byť schválená objednávateľom.

2.12 Dokumentácia aj zdrojové kódy riešenia musia byť odovzdané objednávateľovi spolu so samotným riešením.

2.13 Pokiaľ je súčasťou riešenia aj databáza obsahujúca dôverné údaje:
   a. autentifikačné údaje musia byť uložené iba v podobe osolených hashov (salted hash), pričom použitá hashovacia funkcia by mala byť minimálne sha256
   b. ostatné osobné údaje (adresy, čísla platobných kariet, čísla občianskych preukazov,...) je odporúčané neukladať v čistej podobe, ale chránené šifrovaním[7],

2.14 Musí byť implementované logovanie a logy by mali zaznamenávať minimálne:
   a. (Úspešné aj neúspešné) Prihlásenie a odhlásenie
   b. (Úspešné aj neúspešné) Vytvorenie, modifikáciu alebo zmazanie používateľa alebo skupiny
   c. (Úspešné aj neúspešné) Pokusy pristúpiť k citlivým údajom (údaje klasifikované hornými dvomi klasifikačnými stupňami v rámci organizácie)
   d. (Úspešné aj neúspešné) Pokusy o kritické operácie

2.15 Logy musia byť centrálne ukladané a archivované minimálne 6 mesiacov

5 angl. „Version control system“, napr. git
6 Napr. stack protection, DEP, PIE, nonexecutable stack
7 Je možné použiť aj niektoré „Format-Preserving Encryption“ algoritmy

2.16 Riešenie musí podporovať aj logovanie vo formáte syslog a musí podporovať preposielanie týchto logov na externý syslog server

Testovanie a verifikácia riešenia

2.17 Po ukončení vývoja musí prejsť aplikácia testovaním a verifikáciou:

a. Vývojári by mali overiť aspoň pomocou automatizovaných nástrojov štandardné zraniteľnosti. Malo by prebehnúť minimálne testovanie vstupov (fuzzing) a kontrola práce s pamäťou (memory leaky, memory corruption).
b. Vývojári musia zabezpečiť realizáciu opatrení vyplývajúcich z analýzy rizík vypracovanej pri návrhu riešenia.
c. Musí byť vykonané penetračné testovanie externou organizáciou.
d. Zraniteľnosti a problémy zistené na základe testovania musia byť odstránené a ich oprava musí byť potvrdená opakovaným testovaním.

Nasadenie a prevádzka riešenia

2.18 Hotové riešenie s odstránenými nájdenými zraniteľnosťami musí byť nasadené v prostredí zabezpečenom na základe odporúčaní v kapitolách o zabezpečení služieb a infraštruktúry.

2.19 Musí byť zabezpečené pravidelné monitorovanie nových zraniteľností jednotlivých (najmä externých) súčastí riešenia a pravidelné aplikovanie bezpečnostných záplat vydaných vývojármi, resp. tretími stranami. Aplikovanie týchto záplat musí podliehať opatreniam uvedeným v smernici pre riadenie záplat.

Interná infraštruktúra a vývojové prostredie

Interná infraštruktúra riešenia

2.20 Jednotlivé vrstvy (databázová, aplikačná, prezentačná) by mali byť umiestnené v separátnych segmentoch a komunikácia medzi nimi musí byť filtrovaná

2.21 Jednotlivé servery musia byť hardenované minimálne v rozsahu:

a. Vypnuté všetky nepotrebné procesy a služby
b. Implementovaný host-based firewall, ktorý kontroluje všetku komunikáciu IN aj OUT a je nakonfigurovaný na princípe „least privilege“
c. Všetky administrátorské účty spĺňajú politiku hesiel pre administrátorské účty (Príloha A)
d. Servery a všetok softvér je aktualizovaný minimálne raz za 6 mesiacov, odporúča sa aktualizovať aspoň raz za mesiac.
e. Na serveroch by malo byť implementované anti-malware riešenie, ktoré je centrálne spravované a centrálne logované.
f. Všetky servery majú nastavené lokálny NTP server ako autoritatívny zdroj času a pre preklad doménových mien na IP adresy používajú lokálne DNS servery
g. Všetky zariadenia musia byť hardenované podľa odporúčaní výrobcu.

Vývojové prostredie

2.22 Vo vývojovom prostredí musia byť použité iba nástroje spĺňajúce nasledovné:

a. musia byť získané legálnym spôsobom z dôveryhodných zdrojov,
b. musia byť stále podporované výrobcom (t.j. výrobca poskytuje bezpečnostné aktualizácie) nástroja a nesmú byť označené ako zastarané,
c. musia byť aktualizované minimálne raz za 6 mesiacov a musia byť aplikované bezpečnostné záplaty vydané výrobcom nástroja.

2.23 Vo vývojovom prostredí (vývojárske nástroje a podporné informačné systémy vrátane použitých knižníc tretích strán), v ktorom bude vyvíjané riešenie, musia byť implementované tieto opatrenia:

a. Musia byť implementované príslušné opatrenia na zabezpečenie integrity vyvíjaného riešenia na základe najvyššej požadovanej úrovne ochrany dôvernosti, integrity a dostupnosti informácií, ktoré budú spracovávané vo vyvíjanom riešení.
b. Ak samotné vyvíjané riešenie obsahuje informácie, ktoré je potrebné chrániť z hľadiska dôvernosti[8], musia byť vo vývojovom prostredí implementované opatrenia na zaistenie dôvernosti na základe požadovanej úrovne ochrany dôvernosti týchto údajov.

Mechanizmus kontroly

2.24 Kontrola vykonaných opatrení sa vykonáva dvoma spôsobmi:

a. pri odovzdávaní projektu na mieste dohodnutom medzi objednávateľom a dodávateľom,
b. počas implementácie projektu na mieste, kde prebieha vývoj riešenia.

2.25 Kontrola pri odovzdávaní projektu pozostáva z:

a. kontroly projektovej dokumentácie obsahujúcej minimálne návrh riešenia s popisom jednotlivých súčastí, vývojársku dokumentáciu a dokumentáciu pre používateľov a správcov
b. kontroly analýzy rizík a implementácie navrhnutých opatrení
c. kontroly verzionovanej histórie vývoja projektu pozostávajúcej minimálne z kontroly podpísaných commitov a z kontroly, či zmeny vykonané v danom commite súvisia s jeho popisom.
d. Kontroly zdrojových kódov na použité zastarané/nebezpečné funkcie.
e. Kontroly formátu citlivých údajov v databáze
f. kontroly výsledkov testovania implementovaného riešenia

2.26 Kontrola počas implementácie projektu na mieste, kde prebieha vývoj riešenia, pozostáva z:

a. kontroly použitých vývojárskych nástrojov, ich pôvodu, legálnosti a aktuálnosti
b. kontroly implementovaných opatrení na zabezpečenie integrity vyvíjaného riešenia, prípadne aj jeho dôvernosti
c. kontroly anonymizácie použitých testovacích údajov počas implementácie riešenia
d. kontroly zapnutých bezpečnostných vlastností použitých nástrojov (varovania, ochrany)
e. Kontrolu by mala vykonávať osoba, ktorá je dostatočne technicky zdatná a má minimálne 5 rokov prax v IT odbore, je bezúhonná a nezávislá.

8 Napr. prihlasovacie údaje k databázam.

3 Minimálne požiadavky na zabezpečenie služieb dostupných z externých sietí – Webové aplikácie

Bezpečný návrh

3.1 Webová stránka by mala pozostávať z verejných a neverejných zón a navigácia medzi nimi by nemala umožniť tok citlivých informácií medzi týmito zónami.

3.2 Citlivé informácie by mali byť uchovávané v zašifrovanej podobe.

3.3 Validácia vstupov musí byť vykonávaná na strane servera a odporúča sa, aby bola vykonávaná aj na strane klienta.

3.4 Prezentačný server musí byť umiestnený v zabezpečenej demilitarizovanej zóne (DMZ), ku ktorej môžu pristupovať len autorizované osoby. Aplikačný a databázový server by mali byť umiestnené v internej sieti neprístupnej z Internetu.

3.5 Kód musí byť udržiavaný, prehľadný a dokumentovaný. Viď sekciu 5.11.

3.6 Prezentačná vrstva musí byť oddelená od aplikačnej a databázovej vrstvy.

Šifrovanie

3.7 Webový portál musí byť prístupný prostredníctvom protokolu HTTPS.

3.8 K webovému portálu by sa nemalo pristupovať prostredníctvom HTTP.

3.9 Identita webového portálu musí byť zabezpečená platným, dôveryhodným certifikátom vydaným na doménu, na ktorej je dostupný webový portál.

3.10 Identita webového portálu by mala byť zabezpečená certifikátom s Extended Validation.

3.11 Webový portál nesmie používať nedôveryhodné alebo vypršané SSL/TLS certifikáty.

3.12 Údaje, ktoré sú citlivé z hľadiska integrity alebo dôvernosti sa musia prenášať iba prostredníctvom zašifrovaného spojenia SSL/TLS.

3.13 Citlivé údaje (zvlášť prihlasovacie údaje) musia byť prenášané výhradne prostredníctvom zašifrovaného kanála.

3.14 Webový portál by nemal ukladať citlivé informácie v nezašifrovanej podobe na strane klienta, ani na strane servera.

3.15 Webový portál by nemal vkladať nešifrované zdroje bez SSL/TLS do stránok používajúcich SSL/TLS.

Šifrovacie kľúče a protokoly

3.16 Webový server nesmie podporovať protokoly SSLv2, SSLv3, TLS 1.0 a TLS 1.1.

3.17 Webový server musí podporovať TLS 1.2.

3.18 Webový server by mal podporovať TLS 1.3.

3.19 Webový server by nemal podporovať šifry s kľúčom kratším ako 112 bitov a blokom kratším ako 64bitov.

3.20 Webový server nesmie podporovať NULL ciphers a anonymný Diffie-Hellman algoritmus.

3.21 Webový server nesmie podporovať tzv. Export (EXP) šifry

3.22 Použité šifry a protokoly SSL/TLS by mali byť odolné voči známym typom útokov, ako napríklad: FREAK, BEAST (používanie TLS 1.2, pri TLS 1.0 nepoužívanie šifry s AES), BREACH (Pri SSL/TLS musí byť vypnutá http kompresia), POODLE, LOGJAM, TLS Crime (TLS kompresia by mala byť vypnutá).

3.23 Dĺžka kľúča asymetrickej šifry RSA, DSA v X.509 certifikáte musí byť aspoň 2048 bitov. Toto neplatí pre ECDSA, kedy na dosiahnutie vysokej bezpečnosti postačujú kratšie kľúče – napríklad 256 bitov.

3.24 X.509 certifikáty musia byť hashované bezpečnými hashovacími funkciami (napr. kvôli možnosti kolíznych útokov nesmie byť použitý algoritmus MD5).

3.25 Webový server by mal podporovať šifry, ktoré majú vlastnosť Perfect Forward Secrecy (PFS).

3.26 Webový server by nemal podporovať RC4, DES a 3DES.

3.27 Šifry s CBC módom by mali byť nahradené bezpečnejšími AEAD šiframi. Pri použití CBC šifier je potrebné použiť ďalšiu autentifikáciu, napríklad HMAC (hashovaný autentifikačný kód správ).

3.28 Pre všetky kryptografické operácie musia byť použité kryptograficky silné generátory pseudonáhodných čísel.

3.29 Konfiguráciu odporúčame otestovať v SSL/TLS teste[9].

3.30 Pri správe SSL/TLS je nutné sledovať a v konfigurácii reflektovať aktuálne odporúčania. V prípade použitia WAF/FW pre SSL/TLS preň platia všetky vyššie uvedené požiadavky.

Konfigurácia webového servera

Systém

3.31 Systém, nainštalované aplikácie a frameworky musia byť pravidelne aktualizované z pohľadu bezpečnosti.

3.32 Používané verzie softvéru musia byť podporované, resp. im nesmie končiť podpora.

3.33 Počas doby, kedy prebieha údržba, rozsiahlejšia alebo mimoriadna aktualizácia OS/SW a/alebo nasadzovanie bezpečnostných záplat, by mali byť webové servery oddelené od zvyšku siete organizácie alebo byť umiestnené v izolovaných sieťach.

9 Je možné využiť napríklad bezplatný test od Qualys: https://www.ssllabs.com/ssltest/index.html

3.34 Na serveri musia byť deaktivované všetky nepoužívané služby, frameworky, doplnky a funkcionality.

3.35 Na serveri musia byť zatvorené všetky nepotrebné porty.

3.36 Autentifikácia používateľov na OS servera musí zodpovedať nasledujúcim požiadavkám:

3.37 Nepotrebné implicitné účty musia byť odstránené alebo zneplatnené.

3.38 Neaktívne kontá musia byť zneplatnené.

3.39 Na serveri by mali byť nakonfigurované používateľské skupiny, kontrola prístupu a udeľovanie privilégií by mali byť pre konkrétnych používateľov riadené ich zaradením do týchto skupín.

3.40 Heslo ku kontu musí zodpovedať požiadavkám organizácie na komplexnosť hesiel a má byť znemožnený útok hádaním či hrubou silou, viď príloha dokumentu.

3.41 Právo na vykonávanie systémových úkonov musí byť obmedzené na poverených administrátorov. Tí by sa navyše vzdialene mali prihlasovať iba v restricted režime, ak sa používa RDP (RDP restricted admin).

3.42 Lokálny administrátor webservera musí byť unikátny pre každý webový server.

3.43 Servery s OS Windows buď nesmú byť v doméne alebo musia byť spravované RO doménovým radičom (RODC – read-only domain controller).

Webový server

3.44 Pri inštalácií webového servera a bezprostredne po nej by mali byť vykonané nasledovné kontroly a akcie:

f. SW webového servera má byť inštalovaný na dedikovanom hostiteľskom zariadení alebo na dedikovanom virtualizovanom OS.
g. Musia byť aplikované dostupné záplaty a aktualizácie na eliminovanie známych zraniteľností
h. Pre webový obsah by mal byť vytvorený dedikovaný fyzický disk alebo logická partícia (separátne od OS a SW webového servera).
i. Všetky služby inštalované popri webovom serveri, ktoré nie sú potrebné (napr. FTP server alebo služba vzdialenej administrácie) musia byť vypnuté alebo odstránené.
j. Nepotrebné východzie účty vytvorené pri inštalácií by mali byť odstránené alebo vypnuté.
k. Z webového servera majú byť odstránené testovacie a ukážkové súbory vrátane vykonateľných súborov a skriptov a dokumentácia výrobcu.
l. Odporúčame na server aplikovať hardenovací skript alebo bezpečnostnú šablónu, vhodný pre daný OS a webový server. Info možno čerpať z príručiek dostupných na webstránke CSIRT.SK[10].
m. Banner HTTP služby by mal byť rekonfigurovaný, podľa potreby aj s ďalšími bannermi tak, aby nereportovali typ a verziu webového servera a podkladového OS.

3.45 Webový server by mal podporovať iba HTTP metódy POST a GET.

10 https://www.csirt.gov.sk/informacna-bezpecnost/osvedcene-postupy/nase-publikacie-85a.html

3.46 Webový server nesmú podporovať (musia byť vypnuté) HTTP metódy OPTIONS, TRACK a TRACE.

3.47 Webový server musí byť odolný voči SlowHTTP DoS útokom (limitácia počtu spojení z jednej IP adresy, nastavenie timeoutu na HTTP requesty, implementácia loadbalancerov)

3.48 Z webového servera musia byť odstránené všetky nadbytočné a nepotrebné súbory a zložky, obzvlášť konfiguračné súbory a zálohy, ladiace výstupy, dočasné súbory, nepotrebné zdrojové kódy a zálohy súborov.

3.49 Ladiace funkcionality (napríklad ASP.NET Application Trace) musia byť vypnuté.

3.50 Na serveri musí byť nakonfigurovaný defaultný virtuálny host na obsluhu prístupu na webserver prostredníctvom IP adresy (cez prehliadač). Nesmie byť zobrazovaná defaultná stránka použitého frameworku a pod.

3.51 Webový server musí zobrazovať v prípade chyby servera iba všeobecné chybové hlásenia.

3.52 Webový server by nemal podporovať funkcionalitu listovania adresára (Directory listing, Microsoft IIS tilde directory enumeration).

3.53 Súbor robots.txt nesmie obsahovať odkazy na citlivé zdroje aplikácie (napríklad prihlasovanie administrátora a podobne).

3.54 Webový server by mal byť chránený WAF (web aplikačný firewall) minimálne s nasledujúcou funkcionalitou:

a. Detekcia a prevencia známych útokov (Code injection – SQL, XSS, Command, XPATH, ...),
b. Kontrola používateľských vstupov prostredníctvom whitelistingu a ich prekódovanie do HTML entít alebo podobných bezpečných náhrad.

3.55 Webový server s aplikáciou spracúvajúcou citlivé údajov a/alebo klasifikované informácie, musí byť chránený WAF, ktorého konfigurácia musí byť reštriktívna (kontrola business logiky a pod).

3.56 Na zvýšenie dostupnosti webového servera odporúčame použiť load balancery. Podľa možnosti môžu byť rozšírené o web cache. V prípade podpory web cache nesmú byť cacheované administrátorské stránky, prístupové údaje a podobné citlivé informácie.

3.57 Na zvýšenie dostupnosti webového servera môžu byť ako bezpečnostné brány použité reverzné proxy. Podľa možnosti môžu byť rozšírené o funkcie akcelerácie šifrovania, používateľskej autentifikácie alebo filtrovania obsahu.

3.58 Webový server nesmie podporovať klientom iniciovanú SSL/TLS renegociáciu šifrovacích kľúčov (kvôli DoS útoku).

3.59 Webový server musí dodržiavať negociačný postup negociácie TLS spojenia, popísaný v RFC 5746, kvôli zraniteľnosti Insecure renegociation a riziku útoku typu MitM.

3.60 Webový server by mal podporovať bezpečnú renegociáciu (Secure renegotiation)

3.61 V prípade viacerých virtuálnych hostov musí byť oddelené úložisko cookies minimálne na úrovni adresárov.

Administrácia, logovanie a zálohovanie

3.62 Správcovské rozhrania na všetky služby musia byť dostupné iba z dôveryhodných lokalít (potrebná reštrikcia na lokálne siete).

3.63 Z produkčných systémov musia byť odstránené všetky testovacie a pôvodné účty.

3.64 Všetky servery a syslog servery musia byť synchronizované s dôveryhodným NTP serverom.

3.65 Webové správcovské rozhrania musia byť dostupné iba prostredníctvom SSL/TLS.

3.66 Na serveri musí byť aktívne logovanie:

a. Malo by byť použité kombinované logovanie na ukladanie Transfer logov (formát podporujúci prispôsobenie formátu logu). Ak takýto formát nie je dostupný, je potrebné zabezpečiť aby bolo logované aj hlavičky Referer a User-Agent.
b. Pre každý virtuálny host na fyzickom webserveri by mal existovať separátny log.
c. V logoch musia byť uvedené: timestamp, kedy udalosť nastala, vrátane určenia časovej zóny, verejná IP adresa používateľa, dopytovaná stránka/URL, HTTP kód odpovede servera, veľkosť odpovede servera v bytoch, obsahy hlavičiek User-Agent a Referer. V prípade záznamov o udalostiach súvisiacich s autentifikáciou alebo s činnosťou autentifikovaného používateľa je nutné zaznamenať účet a akciu, aká bola vykonaná.
d. Logy musia byť uchovávané na separátnom zariadení, resp. na separátnej logickej partícii.
e. Na uchovávanie logov musí byť vyhradená dostatočná kapacita.
f. Logy by mali byť byť archivované po dobu stanovenú pravidlami organizácie, minimálne však počas 6 mesiacov.
g. Logy musia byť prezerané v pravidelných intervaloch v závislosti od politiky organizácie, minimálne však raz týždenne. V prípade služieb, ktoré spracúvajú citlivé údaje alebo ich správna činnosť ovplyvňuje kritické aktíva organizácie, by mali byť logy kontrolované denne.

3.67 Webový server musí byť pravidelne zálohovaný nasledovným spôsobom:

a. Zálohovanie servera má byť upravené organizačnými opatreniami organizácie.
b. Archívna záloha musí byť vytvorená minimálne raz ročne.
c. Diferenciálna alebo zmenová záloha webového servera má byť vytvorená na dennej až týždennej báze.
d. Plný backup webového servera by mal byť vytváraný v týždňových až mesačných intervaloch.
e. Zálohy servera by mali byť periodicky archivované na externé médiá.
f. Mala by byť uchovávaná autoritatívna kópia webovej stránky/stránok

Kontrola prístupu OS a webového servera

3.68 Proces webového servera aj proces backendovej databázy musí byť konfigurovaný tak, aby bežal pod unikátnym používateľským kontom s limitovanou množinou privilégií.

3.69 Webový server by mal byť konfigurovaný tak, aby súbory s webovým obsahom boli procesom prislúchajúcim službe webového servera prístupné na čítanie, no nie na zápis. Procesy webového servera by nemali mať právo zápisu do priečinkov, kde je uchovávaný verejný webový obsah (web content).[11]

3.70 OS by mal byť nakonfigurovaný tak, aby proces webového servera mohol vytvárať log záznamy, no nemohol ich čítať.

3.71 OS by mal byť podľa možnosti nakonfigurovaný, aby dočasné súbory vytvorené procesmi webového servera boli obmedzené na určený a vhodne zabezpečený priečinok. Ak je to možné, prístup k dočasným súborom by mal byť obmedzený na procesy, ktoré ich vytvorili.

3.72 Webový obsah a všetky logy ním vytvárané by mali byť umiestnené na separátnom pevnom disku alebo na inej logickej partícii, ako OS a webový server.

3.73 Odporúča sa webový server izolovať od iných procesov použitím prostriedkov ako napríklad chroot, kontajnery, virtualizácia a pod.

3.74 Pre externé skripty a programy, vykonávané ako časť obsahu webového servera by mal byť vytvorený samostatný priečinok (napr. JavaScript knižnice a pod).

3.75 Mal by byť stanovený maximálny počet procesov webového servera a/alebo sieťových spojení, ktoré by server mal povoliť.

3.76 Spúšťanie skriptov, ktoré nie sú výlučne pod kontrolou administratívneho konta, malo by byť zakázané (napr. vytvorením a kontrolou prístupu k separátnemu priečinku, obsahujúcom autorizované skripty).

3.77 Použitie symbolických linkov by malo byť pre procesy webového servera zakázané[12].

3.78 Odporúčame vytvoriť kompletnú maticu prístupov k webovému obsahu (access matrix). V nej by malo byť definované, ktoré súbory a priečinky majú byť prístupné a pre koho.

3.79 V odôvodnených prípadoch odporúčame zaviesť kontrolu proti botom (napr. CAPTCHA, nofollow, filtrovanie kľúčových slov).

HTTP hlavičky a cookies

3.80 Server by mal pri SSL/TLS používať HSTS - HTTP Strict Transport Security. Nastavené by mali byť direktívy:

a. max-age=<číslo> – počet sekúnd, počas ktorých má prehliadač automaticky konvertovať všetky HTTP požiadavky do HTTPS
b. includeSubDomains – indikuje, že všetky subdomény aplikácie musia používať HTTPS

3.81 V odpovediach webového servera sa nesmú nachádzať hlavičky prezrádzajúce použitú technológiu a / alebo jej verziu (Server, X-Powered-By, X-AspNet-Version a pod.)

11 Iba procesy určené na správu webservera (nie procesy bežiacej webovej služby) by mali mať právo zapisovať do súborov s webovým obsahom.

12 Príklad pre konfiguráciu Apache: odstrániť Options FollowSymLinks

3.82 V hlavičkách sa nesmú nachádzať informácie o použitých technológiách, backendových serveroch, internej infraštruktúre, ani bezpečnostných prvkoch.

3.83 Server by mal používať hlavičky:
   a. *X-Frame-Options: SAMEORIGIN* (alebo DENY)
   b. X-XSS-Protection: 1
   c. X-Content-Type-Options: nosniff
   d. Strict-Transport-Security

3.84 V odpovediach webového servera by sa nemali nachádzať hlavičky X-Forwarded-For a HTTP_PROXY

Aplikácia (webový portál)

3.85 Aplikácia musí ošetrovať všetky chyby a výnimky.

3.86 Aplikácia musí zobrazovať v prípade chyby aplikácie iba všeobecné chybové hlásenia.

3.87 V generovanom kóde nesmú byť prítomné komentáre, citlivé informácie a odkazy na vnútorné IP adresy.

3.88 Aplikácia musí pristupovať k ďalším aplikáciám a serverom prostredníctvom doménového mena (nie IP adresy, obzvlášť internej).

3.89 Aplikácia nesmie reflektovať obsahy hlavičiek v odpovedi servera.

3.90 Pre posielanie citlivých a autentifikačných údajov musí byť vynucované HTTPS spojenie.

3.91 Aplikácia nesmie ukladať citlivé údaje (napríklad identifikátor relácie) v URL adrese. V prípade zakázania cookies v prehliadači musí stránka zobraziť hlásenie o nutnosti použitia cookies (ak sa používajú).

3.92 Aplikácia by nemala používať odkazy na externé zdroje (zdroje mimo správy prevádzkovateľa alebo inštitúcie verejnej správy na SR).

3.93 Aplikácie nesmie používať odkazy na nedôveryhodné externé zdroje.

3.94 Všetky činnosti privilegovaných používateľov a administrátorov by mali byť zaznamenávané do log súborov prostredníctvom vzdialených logovacích serverov (syslog, Windows Event Forward).

3.95 Aplikácia nesmie používať funkciu eval() alebo jej alternatívy.

3.96 Z aplikácie musia byť odstránené všetky ladiace výstupy, dočasné súbory, nepotrebné zdrojové kódy a zálohy súborov.

Autentifikácia a autorizácia

3.97 Aplikácia musí pre všetky autorizačné mechanizmy implementovať politiku, pri ktorej je zakázané všetko, čo nie je explicitne povolené (default-deny).

3.98 Aplikácia musí vyžadovať autentifikáciu pre každú privilegovanú operáciu (napr. meno a heslo na prvotné prihlásenie, token).

3.99 Aplikácia musí implementovať autorizáciu a autentifikáciu na strane servera.

3.100 Musia byť odstránené všetky testovacie a pôvodné účty z produkčných systémov.

3.101 Pre všetky citlivé operácie musia byť implementované anti-CSRF tokeny, ktoré musia byť pri vykonaní operácie overované.

3.102 Pre webové aplikácie, ku ktorým je na prístup nutná autentifikácia, je nutné zabezpečiť, aby žiadna webová stránka, ktorá má byť prístupné až po autentifikácii, nebola dostupná bez vykonania kompletného procesu autentifikácie.

3.103 Autentifikácia musí prebiehať prostredníctvom protokolu HTTPS.

3.104 Aplikácia musí vyžadovať používanie silných hesiel, viď Príloha A – Politika hesiel.

3.105 V prípade použitia iniciálnych náhodne generovaných hesiel pre nového používateľa musí aplikácia pri prvom prihlásení vyžadovať zmenu tohto hesla, v súlade s definovanými pravidlami pre tvorbu hesiel.

3.106 Aplikácia musí umožňovať administrátorom i používateľom zmeniť ich heslo.

3.107 Aplikácia musí vyžadovať pravidelnú zmenu hesla, musí byť nastavený minimálny a maximálny interval na zmenu hesla.

3.108 Aplikácia musí pri zmene hesla vyžadovať zadanie starého hesla.

3.109 Aplikácia musí pri zmene hesla vyžadovať opakované zadanie nového hesla (2 krát), pričom nové zadané heslá sa musia zhodovať.

3.110 Odporúčame pri zmene hesla používať viacfaktorové potvrdenie, napríklad Out-Of-Band kanálom (mail, SMS, ...)

3.111 Aplikácia musí po zmene hesla vydať nový identifikátor relácie, cez ktorú zmena hesla nastala. Ostatné relácie príslušného používateľa musia byť zneplatnené.

3.112 Aplikácia by mala pri zmene hesla notifikovať používateľa prostredníctvom Out-Of-Band kanála.

3.113 Aplikácia musí uložené heslá hashovať prostredníctvom štandardných kryptografických hashovacích funkcií a musí používať soľ (angl. salt).

3.114 Aplikácia musí implementovať funkcionalitu pre odhlásenie (log-out) aj pre automatické odhlásenie po istej dobe nečinnosti. Funkcia odhlásenia má byť jednoducho identifikovateľná a dostupná z každej stránky, prístupnej po autentifikácii.

3.115 Aplikácia musí po odhlásení zneplatniť všetky relácie daného používateľa.

3.116 Odporúča sa, aby aplikácia podporovala simultánne paralelné prihlásenie k jednému účtu iba z jednej verejnej IP adresy. Odporúča sa, aby aplikácia pri zmene verejnej IP adresy prihláseného používateľa požadovala reautentifikáciu[13].

3.117 Odporúča sa naviazanie relácie na parameter User-Agent.

3.118 Aplikácia musí podporovať spustenie mechanizmu zamknutia účtu (lockout) po istom počte neúspešných pokusov (maximálne 5) o prihlásenie.

3.119 Zamknutie účtu po stanovenom počte neúspešných pokusov o prihlásenie musí trvať aspoň 10 minút.

3.120 Zamknutie účtu po stanovenom počte neúspešných pokusov o prihlásenie do kritického systému by malo trvať aspoň hodinu.

3.121 Je nutné vytvárať log záznamy všetkých pokusov o autentifikáciu (log-in, log-out, neúspešný log-in, lockout konta, žiadosť o zmenu hesla).

3.122 V prípade zamknutia účtu by aplikácia mala notifikovať zodpovednú osobu, resp. administrátora aplikácie.

3.123 Pre privilegované účty sa musia používať používateľské mená, ktoré nie je možné jednoducho dedukovať (napr. štandardné loginy ako *admin*, *administrator, user* a pod, názov alebo typ aplikácie, kombinácie uvedených a pod.).

3.124 Aplikácia nesmie pre kritické systémy umožniť funkcionalitu zapamätania si hesla.

3.125 Používateľské kontá by mali byť po určitej dobe nečinnosti znefunkčnené.

3.126 Používateľské kontá, ktoré neboli použité do 3 mesiacov od ich vytvorenia (používateľ sa počas danej doby nikdy neprihlásil), by mali byť deaktivované.

3.127 Každý používateľ a administrátor musia mať jedinečné ID.

3.128 Aplikácia nesmie umožniť vytváranie účtov s používateľským menom podobným administrátorským či servisným kontám. Napríklad: *admin, administrator, helpdesk, support* a pod.

3.129 Aplikácia musí korektne inštruovať prehliadač, aby neukladal citlivé informácie, prenášané prostredníctvom HTTPS, do cache (a aby neboli bez kontroly opäť prístupné z histórie prehliadania) minimálne v rozsahu:

a. Server musí nastavovať vo svojich odpovediach hlavičky
   - Cache-Control: no-cache, no-store, private, must-re-validate, max-age=0, no-transform
   - Expires: 0
   - Pragma: no-cache

13 Upozorňujeme, že funkcionalita zviazania zdrojovej IP adresy s reláciou je problematická ak k aplikácii pristupujú klienti, ktorých ISP dynamicky mení zdrojovú verejnú IP adresu. Taktiež môže byť problematická ak sa používa IPv6.

Používateľské vstupy

3.130 Všetky používateľské vstupy musia byť kontrolované na strane servera prostredníctvom whitelistov alebo regulárnych výrazov v kontexte, v ktorom sú použité.

3.131 Aplikácia musí brať ako vstupy a primerane ošetrovať všetky používateľom ovplyvniteľné časti dopytu, vrátane HTTP hlavičiek, URL, Cookies a pod. Bez ošetrenia nesmú byť reflektované v odpovedi servera. Napríklad:

a. Aplikácia musí byť odolná voči HTTP Spitting/Smuggling útokom
b. Aplikácia by mala byť odolná voči HTTP Parameter Pollution (HPP) útokom.
c. Aplikácia/webový server musí byť odolný voči Host Header útoku.

3.132 Aplikácia by mala používať parametrizované SQL požiadavky (queries), tzv. prepared statements.

3.133 Aplikácia nesmie na tvorenie SQL dotazov využívať používateľské vstupy bez ich dôkladnej kontroly a ošetrenia.

3.134 Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím. Minimálne:

a. Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v názvoch súborov a zložiek.
b. Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v akomkoľvek skripte, databázovom dopyte alebo parametri príkazu operačného systému.
c. Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v kontexte HTML.
d. Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v kontexte JavaScript.
e. Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v kontexte REST API.
f. Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v XML dokumentoch.
g. Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v XPath požiadavkách (query).
h. Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v XSL(T) style sheets.
i. Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v SSI (Server-Side Inclusion statements) príkazoch, ak je použitie SSI nutné a povolené.
j. Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v HTTP hlavičkách.
k. Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v HTTP parametroch.
l. Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v LDAP požiadavkách.
m. Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v regulárnych výrazoch.
n. Aplikácia musí ošetrovať vstupy/dátové prúdy prechádzajúce medzi modulmi aplikácie.

Relácie

3.135 Aplikácia by mala používať CSRF tokeny o veľkosti aspoň 128 bitov.

3.136 Aplikácia by nemala povoliť požiadavky spôsobujúce zmenu údajov, alebo citlivú operáciu bez platného CSRF tokenu.

3.137 Aplikácia nesmie povoliť požiadavky na privilegované operácie bez platného CSRF tokenu.

3.138 Na generovanie CSRF tokenov musí aplikácia používať kryptograficky silný generátor pseudonáhodných čísel.

3.139 Pri prihlásení musí aplikácia znovu vygenerovať nový identifikátor relácie. Identifikátor predchádzajúcej neautentifikovanej relácie musí byť zneplatnený.

3.140 Pri zmene prihlasovacích údajov (používateľské meno, heslo) musí aplikácia znovu vygenerovať identifikátor relácie.

3.141 Pri zmene prihlasovacích údajov (používateľské meno, heslo) musí aplikácia zneplatniť ostatné relácie príslušného používateľa.

3.142 Pre relačné (session) cookies musí aplikácia nastaviť Secure flag.

3.143 Pre relačné (session) cookies musí aplikácia nastaviť HttpOnly flag.

3.144 Pre relačné (session) cookies musí aplikácia nastaviť reštriktívnu doménu.

3.145 Pre relačné (session) cookies musí aplikácia nastaviť reštriktívnu cestu (path).

3.146 Pre generovanie relačných identifikátorov musí aplikácia používať kryptograficky silné generátory pseudonáhodných čísel.

3.147 Aplikácia by mala používať relačné identifikátory o veľkosti aspoň 128 bitov.

3.148 Aplikácia musí zamietať neznáme relačné identifikátory zo strany klienta.

3.149 Relačné identifikátory musí aplikácia prenášať iba cez zabezpečené pripojenia. Aplikácia musí vynucovať periodickú exspiráciu a zneplatnenie relácií.

Nahrávanie súborov

3.150 Aplikácia musí nahrávané súbory ukladať mimo koreňového súboru pre dokumenty (document root) na separátnu partíciu disku (inú, ako je vyhradené na zápis logov), kde súčasne nesmie byť možnosť listovania adresára a nesmie byť možnosť interpretovať nahraté súbory ako napríklad skripty (PHP, ASP, JSP, ...).

3.151 Aplikácia nesmie spúšťať a vyhodnocovať (evaluate) nahraté súbory.

3.152 Aplikácia musí vynucovať limit pre veľkosť nahratých súborov.

3.153 Aplikácia by mala obmedzovať počet súborov nahraných za hodinu.

3.154 Aplikácia musí umožniť nahrávanie iba špecifických typov súborov a kontrolovať nielen ich príponu, ale aj MIME typ.

3.155 Aplikácia by mala nahrávané súbory kontrolovať na prítomnosť škodlivého kódu prostredníctvom antimalware riešenia.

3.156 Nahrávané súbory by sa nemali ukladať pod pôvodným názvom.

Obsah

3.157 Aplikácia by mala pre všetky poskytované zdroje explicitne definovať typ obsahu.

3.158 Aplikácia by mala pre všetky poskytované stránky definovať „character set“.

3.159 Zabezpečenie aktívneho obsahu (skripty, spustiteľné súbory):

a. Právo na čítanie a zápis do súborového systému by malo byť limitované alebo zakázané.
b. Mala by byť povolená žiadna alebo len limitovaná interakcia s inými programami.
c. Nemala by byť potrebná žiadna akcia so SUID privilégiami (OS UNIX/Linux).
d. Skripty by pri spúšťaní externých programov mali používať absolútne cesty alebo nepoužívať žiadne cesty a spoliehať sa na premennú PATH, pričom tá musí obsahovať len bezpečné adresáre.
e. Žiadne priečinky nesmú mať súčasne práva na zápis a vykonávanie.
f. Spustiteľné súbory by mali byť umiestnené vo vyhradených priečinkoch.
g. SSI (Server-Side Inclusion) by mali byť zakázané, resp. nie je možné ich spúšťať.

3.160 Spracovanie XML

a. Aplikácia nesmie podporovať XML External entity expansion.
b. Aplikácia nesmie podporovať parsovanie XML External DTD.
c. Aplikácia nesmie podporovať všetky nadbytočné alebo nebezpečné XML rozšírenia.
d. Aplikácia by mala používať XML parser, ktorý neexpanduje entity rekurzívne.

Rôzne

3.161 Aplikácia by nemala podporovať presmerovanie na používateľom poskytnuté externé umiestnenia.

3.162 Aplikácia by mala obmedziť (krížový) prístup k (cudzím) doménam prostredníctvom whitelistingu.

a. Ak je na riadenie prístupu medzi doménami používané CORS (Cross Origin Resource Sharing), konfigurácia by mala byť obmedzená na dôveryhodné domény. Napr. nemala by byť použitá direktíva *Access-Control-Allow-Origin:**
b. Ak aplikácia používa na kontrolu prístupu k zdrojom na externých doménach súbory crossdomain.xml a/alebo clientaccesspolicy.xml, obsah by mal mať obmedzený na nutné domény, porty a protokoly. Nemali by byť používané nadmerne voľné pravidlá s „*“. Crossdomain.xml a clientaccesspolicy.xml nesmú byť prístupné koncovému používateľovi.

3.163 Aplikácia by mala pre všetky emailové funkcionality implementovať rate limiting.

3.164 Aplikácia by mala pre všetky funkcionality vyžadujúce veľa zdrojov (napríklad CPU čas) implementovať rate limiting.

3.165 Pri implementácii rate limitingu sa musí brať ohľad na predchádzanie neúmyselnému odopretiu služby.

Mechanizmus kontroly

3.166 Bezpečnosť webových aplikácií je nutné pravidelne preverovať externým skenom zraniteľností.

3.167 Externým penetračným testom by mal prejsť každý projekt ešte pred nasadením do ostrej prevádzky.

3.168 Komplexný kontrolný externý penetračný test odporúčame vykonať raz ročne.

3.169 V prípade, že webový server sa nachádza v infraštruktúre organizácie, bezpečnosť podkladového OS má byť preverovaná tak, ako je uvedené v kapitole o zabezpečení internej infraštruktúry organizácie.

3.170 Bezpečnostný audit servera a aplikácie by mal byť vykonaný minimálne raz ročne.

4 Minimálne požiadavky na zabezpečenie infraštruktúry

V tejto kapitole sú uvedené požiadavky na zabezpečenie infraštruktúry, ktoré sú spoločné pre internú infraštruktúru aj pre externú infraštruktúru.

Výnimkou k požiadavkám uvedeným v tomto dokumente je labová sieť – t.j. testovacia sieť určená na testovanie nových technológií. Takáto sieť – ak sa používa – by mala byť fyzicky oddelená od siete organizácie a mala by využívať vlastné pripojenie do externých sietí. Nesmú existovať prepojenia medzi koncovými stanicami internej siete organizácie a labovou sieťou.

Všeobecné požiadavky

4.1 Prístup k službe musí byť filtrovaný aspoň na centrálnom FW, na lokálnom FW systému a v konfigurácii danej služby.

4.2 Všetok softvér a firmvér musí byť pravidelne aktualizovaný. Musia byť dodržané tieto princípy:

a. Aktualizácia systémov musí prebiehať prostredníctvom kanála zabezpečujúceho integritu a autentickosť.
b. Odporúča sa vopred otestovať vplyv aktualizácii na systém na testovacom zariadení.
c. V prípade infraštruktúry Windows a použitia lokálneho aktualizačného servera (WSUS) je nutné implementovať šifrovanie aj metadát a implementovať používanie certifikátov podpísaných dôveryhodnou certifikačnou autoritou.

4.3 Na zariadeniach musí byť zapnuté minimálna množina služieb potrebná pre správne fungovanie. Všetka nepotrebná funkcionalita by mala byť neimplementovaná/neinštalovaná - musí byť aspoň vypnutá.

4.4 Konfiguračné súbory musia byť zabezpečené minimálne takto:

a. Konfiguračné súbory by mali byť modifikovateľné len správcom.
b. Súbory obsahujúce heslá, kryptografické kľúče a iné tajomstvá musia byť modifikovateľné a čitateľné len oprávnenými používateľmi.

4.5 Správcovské a monitorovacie rozhrania sieťových prvkov a serverov nesmú byť prístupné priamo z externej siete. Správcovské a monitorovacie rozhrania musia byť prístupné len zo špecifikovaných sietí (napr. administrátorská sieť).

4.6 Správcovské rozhrania služieb by nemali byť priamo prístupné z externej siete. V prípade potreby dostupnosti takýchto rozhraní sa odporúča využiť správcovská VPN. V prípade nutnosti sprístupnenia priamo z externej siete je nutné sprístupniť to len dočasne pre špecifikované zdrojové IP adresy a odporúča sa využiť dodatočnú formu autentifikácie ako je napríklad použitie klientskych certifikátov.

4.7 Správcovské rozhrania zariadení a služieb by nemali byť prístupné cez nešifrované kanály. Pre prístup na správcovské rozhrania sa odporúča využívať autentifikáciu pomocou asymetrickej kryptografie (napr. RSA kľúče, alebo klientske certifikáty). Mal by byť nakonfigurovaný

maximálny timeout pre platnosť neaktívneho spojenia. Musia byť logované všetky pokusy o prihlásenie na správcovské rozhrania.

4.8 Všetky autentifikačné mechanizmy musia používať silnú autentifikáciu. V prípade hesiel a zdieľaných tajomstiev platia požiadavky na komplexnosť a dĺžku hesla, v prípade certifikátov a kryptografických kľúčov platia požiadavky na minimálnu dĺžku a použitý hashovací algoritmus (požiadavky sú uvedené v prílohe A).

4.9 Ak sa nepoužíva IPv6, musí byť vypnutá podpora IPv6 v celej infraštruktúre. To znamená, že koncové stanice musia mať vypnutý IPv6 stack, switche a smerovače nesmú spracovávať a preposielať IPv6, na sieťových firewalloch musia byť nastavené pravidlá zahadzujúce IPv6 komunikáciu vrátane IPv6 komunikácie tunelovanej cez IPv4.

4.10 Ak sa používa IPv6, všetky bezpečnostné prvky (napr. FW, IPS, ACL) filtrujúce komunikáciu musia rozoznávať a kontrolovať aj IPv6.

4.11 Všetky koncové zariadenia by mali byť nakonfigurované tak, aby nespracovávali ICMP Redirect a ICMPv6 Redirect správy.

4.12 Fyzická bezpečnosť zariadení musí byť zabezpečená aspoň v tomto rozsahu:

a. Prístup k zariadeniu musí mať len autorizovaný personál (aspoň na úrovni prístupu do miestnosti, v prípade zdieľaných miestností aj na úrovni stojanového rozvádzača).
b. Musia byť zabezpečené vhodné prevádzkové podmienky zabezpečujúce stabilitu systému určené na základe odporúčaní výrobcu. Minimálne musí byť kontrolovaná teplota, vlhkosť, prašnosť a bezpečný prívod elektrickej energie.

Konfigurácia sieťovej infraštruktúry

4.13 Nepoužívaný verejný IP rozsah organizácie by mal byť null-routed (t.j. nesmerovaný .

4.14 Servery poskytujúce služby či už do externej alebo internej siete musia mať smerom do externej siete povolenú len potrebnú komunikáciu na základe whitelistingu.

4.15 Správcovské rozhrania sieťových prvkov by mali byť dostupné len cez dedikované manažmentové rozhranie a z fyzicky oddelenej správcovskej siete.

4.16 Pre prístup by nemal byť použitý telnet ani HTTP, odporúča sa využívať SSHv2 alebo HTTPS. Pri SSHv2 musí byť zakázaná spätná kompatibilita (SSH v1.99). Pre zálohovanie by nemalo byť použité TFTP, odporúča sa SCP alebo SFTP.

4.17 Pre autentifikáciu prístupov sa odporúča implementovať autentifikačný server (napríklad TACACS+ alebo Radius). Lokálne heslo nakonfigurované pre offline prístup by malo byť unikátne pre každé zariadenie a prístupné len v prípade potreby a nedostupnosti služby autentifikačného servera. V rámci infraštruktúry by nemali byť používané zdieľané administrátorské heslá. Kedykoľvek je to možné, musia byť heslá v konfigurácii zariadenia uložené v šifrovanej / hashovanej forme. Pričom hash nesmie byť reverzibilný (ako je napr. Cisco password type 7).

4.18 Aktívne sieťové prvky musia byť pred nasadením do prevádzky hardenované a to aspoň v rozsahu:

a. Vypnutie nepotrebných služieb (napríklad bootp, CDP, DHCP klient, HTTP server, SNMP a iné).
b. Nastavenie manažment rozhrania, prístupových metód a ACL.
c. Vypnutie password-recovery precedúry.
d. Nastavenie žiadanej úrovne logovania bezpečnostných udalostí.
e. Odporúča sa hardenovať podľa odporúčaní výrobcu.

4.19 Kontrolné správy vymieňané sieťovými prvkami zapojenými v móde "high availability" (napr. hraničné smerovače vo failover móde) musia mať zabezpečenú autentickosť a mali by mať zabezpečenú aj dôvernosť (napríklad využitím silného failover kľúča). Taktiež by mali na komunikáciu používať separátny na to určený kanál.

4.20 Komunikácia v rámci použitých smerovacích protokolov musí byť autentifikovaná.

4.21 Pri každej zmene v sieťovej infraštruktúre je nutné aktualizovať ACL a FW pravidlá.

4.22 Odporúča sa dokumentovať účel a potrebu FW pravidiel a ACL pravidiel v komentároch daných pravidiel.

4.23 Ak sa používa IPv6, musia byť aplikované IPv6 ACL a FW pravidlá v celej infraštruktúre a musia brať ohľad na špecifiká IPv6. IPv6 infraštruktúra musí byť hardenovaná minimálne v rozsahu:

a. princípy architektúry siete a filtrovania komunikácie na základe „least priviledge“ sú obdobné ako pre IPv4 a mali by byť dodržané základné pravidlá uvedené v tomto dokumente
b. Hraničné routre musia byť nakonfigurovaná podľa pravidiel uvedených pre IPv4 routre s týmto rozdielom: musia byť schopné odosielať ICMPv6 Packet Too Big správu.
c. Mal by byť implementovaný anti-bogon filtering na vstupoch z externých sietí.
d. V sieti by nemali byť používané ani povolené „deprecated“ IPv6 funkcionality. Nesmie sa používať Extension Header Routing type 0 a musí byť zahadzovaný na sieťových firewalloch.
e. Nemali by byť používané ani preposielané žiadne IPv6 Extension Headers s výnimkou ESP a AH ak je používaný IPSec.
f. Klientské stanice nesmú byť prístupné priamo z Externých sietí.
g. Klientské stanice by mali pristupovať do Externých sietí cez proxy
h. Sieťové firewally musia byť schopné mapovať k povoleným spojeniam prípadné vracajúce sa ICMPv6 Error správy. Sieťové firewally na rozhraniach vnútornych a externých sietí musia rozoznávať a filtrovať IPv6 extension headers.
i. Pri prideľovaní IPv6 adries serverom by mal byť dodržaný princíp riedkej alokácie adries. Ak sa používa DHCPv6 pre klientské počítače, odporúča sa využiť princíp riedkej alokácie adries.
j. Pakety s multicastovou zdrojovou IPv6 adresou musia byť zahadzované.
k. Smerovače musia rešpektovať IPv6 unicast aj multicast scope (napr. paket s Link Local zdrojovou IP adresou nesmie byť smerovaný ďalej)
l. Zariadenia v sieti by nemali odpovedať na ICMPv6 echo request s multicastovou cieľovou IPv6 adresou

m. Ak sa nepoužíva QoS, odporúča sa normalizácia polí Flow Label a ToS v IPv6 hlavičkách spojení s Externými sieťami.

Zabezpečenie servera

4.24 Odporúča sa aby každá služba bežala na samostatnom serveri. Ak je potrebné využiť jeden server pre viacej služieb, musia na ňom bežať služby s podobným určením a požiadavkami na hardvérovú a softvérovú konfiguráciu.

4.25 Všetky servery dostupné z externých sietí musia byť hardenované podľa odporúčaní výrobcu. Všetky servery by mali byť hardenované podľa odporúčaní výrobcu.

4.26 Každá sieťovo prístupná služba by mala byť spúšťaná pod dedikovaným používateľom a tento používateľ by mal mať obmedzené práva v rámci systému na nutné minimum. Všetky ostatné služby a aplikácie bežiace na danom serveri by mali bežať s právami obmedzenými na nutné minimum.

4.27 Všetky používateľom kontrolované vstupy by mali byť ukladané na diskovú partíciu inú od systémovej partície (na ktorej sú súbory OS a aplikácií).

4.28 Pri inštalovaní nového servera sa odporúča začínať od minimálnej inštalácie a doinštalovať programy a služby podľa potreby.

4.29 Pri inštalovaní nového servera alebo nasadzovaní novej služby je nutné vykonať to v separátnej sieti (VLAN) na to určenej. Do tejto siete a z tejto siete musí byť povolená len minimálna nutná komunikácia na správcovský prístup, inštaláciu aktualizácii a testovanie služby.

4.30 Servery s OS Windows v DMZ (so službami dostupnými z externých sietí) musia byť spravované RO doménovým radičom (RODC – read-only domain controller), alebo ak to nie je možné, tak nesmú byť zaradené v doméne.

4.31 Na kritických serveroch s OS Windows ako sú doménové kontrolery, DNS servery apod. musí byť implementovaný whitelisting spúšťateľných súborov (napr. Applocker od Microsoft) tak, aby bolo možné spúšťať iba dôveryhodné povolené aplikácie.

4.32 Na kritických serveroch s OS Windows ako sú doménové kontrolery, DNS servery apod. musí byť nainštalovaný a nakonfigurovaný nástroj EMET (od Microsoft) so zapnutými všetkými ochranami, ktoré je možné zapnúť. Ak pre niektorý používaný program nie je možné zapnúť všetky ochrany, odporúča sa prehodnotiť potrebu jeho používania.

4.33 Na kritických serveroch ako sú servery s externe dostupnými službami, doménové kontrolery, DNS servery apod, by mali byť aktualizácie a mitigácie pre kritické zraniteľnosti (s vysokým dopadom) aplikované do 72 hodín od ich zverejnenia.

Monitorovanie a logovanie

4.34 V prípade neobvyklej udalosti by mal byť notifikovaný systémový administrátor a to minimálne v týchto prípadoch:

a. blížiace sa zaplnenie kapacity úložného priestoru
b. neštandardne vysoká záťaž systému (load)
c. detegovaná neobvyklá bezpečnostná udalosť

4.35 Logy by mali byť posielané zabezpečeným kanálom a/alebo dedikovanou správcovskou linkou.

4.36 Odporúča sa implementovať unifikovaný centrálny monitorovací systém s nastavenými metrikami pre každé monitorované zariadenie/systém. Príklady nastavenia metrík: upozornenie e-mailom pri 80% zaplnenia diskovej partície, SMS alert pri 95% zaplnení diskovej partície, upozornenie pri 50% využití CPU počas 5 minút, SMS alert pri nedostupnosti kritickej služby viac ako 5 minút.

4.37 Musia byť monitorované všetky centrálne sieťové prvky a servery a služby prístupné do externých sietí ako aj kritické interné servery a služby. Mali by byť monitorované všetky sieťové prvky a servery a služby.

4.38 Musí byť určený personál zodpovedný za monitorovanie logov a upozornení a vykonanie potrebnej akcie v prípade incidentu. Odporúča sa vytvoriť prvú líniu operátorov, ktorý budú obsluhovať monitorovací systém a korigovať nápravné opatrenia.

4.39 Odporúča sa nastaviť monitorovací systém tak aby v prípade vážnych udalostí produkoval aj upozornenie ce "out-of-band" kanál (napríklad e-mail a SMS).

4.40 Logy musia obsahovať korektné informácie o dátume, čase a použitej časovej zóne. Pre korektné nastavenie času sa odporúča nastaviť synchornizáciu s dôveryhodným NTP serverom. Odporúča sa využiť autentifikovanú NTP synchronizáciu.

4.41 Granularita logovania musí zodpovedať požiadavkám danej služby alebo zariadenia a jeho kritickosti.

4.42 Logovanie musí byť nastavené tak, aby prípadné zaplnenie logovacieho miesta neovplyvnilo stabilitu OS. Možné opatrenia: samostatná disková partícia, rotovanie logov a maximálna veľkosť logov.

4.43 Logy z kritických služieb a serverov musia byť synchronizované na samostatné logovacie zariadenie.

4.44 Logovacie súbory by mali byť zabezpečené aspoň takýmto spôsobom:

a. Mali by byť čitateľné len administrátorom.
b. Nemali by byť prepisovateľné a vymazateľné (mal by byť možný len zápis na koniec súboru)[14].
c. Odporúča sa komprimovať a šifrovať archivované logovacie súbory. Pri ručnej archivácii sa odporúča aj podpisovať logovacie súbory.

14 Upozorňujeme, že pri používaní logrotate je potrebná dodatočná konfigurácia.

4.45 Bezpečnostný monitoring by mal zbierať aspoň tieto informácie z pracovných staníc a serverov (v zátvorkach uvádzame príklady Event ID pre OS Windows 6.0+)

a. Vytvorenie nového používateľa (Windows Security event ID 4720, 4724, 4738)

b. Pridanie používateľa do privilegovanej skupiny (Windows Security Event ID 4728, 4732)

c. informácie o zmazaní logov (Windows Security Event ID 1102)

d. Nainštalovanie novej služby (Windows System Event ID 7045, 7030)

e. Vypnutie lokálneho firewallu (Windows Event ID 2003)

f. Nepovolenie spustenia vykonateľného súboru, kvôli whitelisting pravidlu (Windows Applocker: Event ID 8004)

g. Detekcia a zabránenie vykonania potenciálne škodlivého kódu, alebo vypnutie programu anti-exploit komponentom (Microsoft EMET: Windows Application Log Provider EMET ID 2)

h. Detekcia škodlivého kódu antimalware riešením

i. informácie o všetkých spustených procesoch aj s plným príkazovým riadkom

j. odporúča sa implementovať logovanie prístupu k citlivým aktívam (napríklad súbory, riadky databázovej tabuľky apod.)

4.46 Odporúča sa aby bezpečnostný monitoring zbieral aspoň tieto informácie zo sieťového monitoringu:

a. skenovanie sietí a portov, pokus o prístup do nevyužitého IP rozsahu organizácie, pokus o prístup na honeypot

b. história dotazov na DNS mená a vyhodnocovanie podozrivých DNS mien (napríklad na základe entropie, reputačných databáz, alebo štatistiky využitia)

4.47 Odporúča sa do citlivých interných sietí (napríklad VLAN interných serverov) umiestniť honeypot (t.j. nepoužívaný počítač, ktorého účelom je detegovať prístomnosť útočníka v sieti) a pravidelne alebo automaticky vyhodnocovať, či nebol detegovaný pokus o prístup.

4.48 Informácie získané bezpečnostným monitoringom by mali byť vyhodnocované operátorom a v prípade detegovanej zmeny, ktorá nie je zaznamenaná Zmenovým riadením (CM – Change management) by mal byť okamžite spsutený proces riešenia bezpečnostného incidentu.

5 Minimálne požiadavky na zabezpečenie externej infraštruktúry

Nutnou súčasťou požiadaviek na zabezpečenie externej infraštruktúry sú aj požiadavky v kapitole „Minimálne požiadavky na zabezpečenie infraštruktúry organizácie“.

Všeobecné požiadavky

5.1 Pre servery s verejne prístupnými službami je nutné aplikovať bezpečnostné aktualizácie prioritne a to hneď ako je to možné (minimálne raz za mesiac).

5.2 Verejne prístupné zdroje (web, bannery, DNS apod.) nesmú obsahovať informácie o použitých technológiách, vnútorných IP adresách a použitých TCP/UDP portoch.

5.3 Verejne dostupné služby by mali byť dostupné takým spôsobom, ktorý umožňuje používateľovi overiť identitu služby a autentickosť údajov (napr. web, VPN). Odporúča sa verejne prístupné služby sprístupňovať len takýmto spôsobom.

Konfigurácia sieťovej infraštruktúry

5.4 Služby dostupné verejnosti (napríklad webové servery) by mali používať iné pripojenie do Internetu ako to, ktoré používa organizácia na prístup k Internetu alebo iným externým sieťam.

5.5 ACL na hraničných sieťových prvkoch aplikované na všetku komunikáciu prichádzajúcu z externých sietí musí obsahovať aspoň:

a. Zahadzovať komunikáciu so zdrojovými IP adresami z rozsahu RFC 1918 (privátne IP adresy)
b. Filtrovať komunikáciu z rozsahu RFC 3330 (IP adresy rezervované pre špeciálne použitie)
c. Zahadzovať komunikáciu so zdrojovými IP adresami z rozsahu používaného v sieti organizácie
d. Zahadzovať ICMP protokol s výnimkou ICMP echo request. Echo request musí byť povolený len ak je to potrebné a len do DMZ sietí. Taktiež preň musí byť implementovaný rate-limiting
e. odporúča sa implementovať anti-bogon filtering (*oficiálna databáza je udržiavaná na https://www.team-cymru.org/bogon-reference.html)

5.6 Hraničné sieťové prvky by nemali nijak odpovedať na pokusy o pripojenie na neexistujúci TCP/UDP port. Nesmú odosielať správy "ICMP unreachable".

5.7 Z externých sietí nesmie byť povolený ICMP protokol. Výnimkou môže byť povolenie "ICMP echo request" na konkrétne servery v DMZ, pričom musí byť limitovaný počet požiadaviek za daný čas.

5.8 Mal by byť implementovaný Unicast Reverse Path Forwarding.

5.9 Všetky servery so službami priamo prístupnými z externých sietí musia byť v samostatných sieťových segmentoch (DMZ). V rovnakom segmente by mali byť iba servery s rovnakými bezpečnostnými požiadavkami a podobným účelom.

Firewall

5.10 Všetky prepoje medzi segmentami a externými sieťami musia byť chránené firewallom a všetky spojenia (IN aj OUT) musia byť povoľované iba na princípe least privilege.

5.11 Smerom do vnútra musia byť povolené len špecifikované služby umiestnené v DMZ (politika "default deny")

5.12 Smerom do externých sieti by mala byť povolená len špecifikovaná komunikácia (pre interné siete by to malo byť len HTTP a HTTPS).

5.13 Všetky spojenia do externých sietí musia byť smerované cez dedikovaný sieťový firewall. Všetky spojenia do externých sietí okrem VoIP by mali byť smerované aj cez IPS (ak je IPS použité) - výnimkou je VoIP, pre ktoré sa toto odporúča ak to výkon a funkcionalita IPS dovoľuje.

5.14 Musí byť obmedzená táto komunikácia:

a. DNS požiadavky smerom do externých sietí (dport UDP/TCP 53) môžu iniciovať len autorizované rekurzívne DNS servery.
b. SMTP správy smerom do externých sietí (dport TCP 25) môžu posielať len autorizované (t.j. na to určené) SMTP servery.
c. SMTP smerom do externých sietí môžu iniciovať len autorizované SMTP servery.
d. Odporúča sa nepovoľovať smerom do externých sietí komunikáciu na TCP/445 (SMB), TCP/6697 (IRC).

Ochrana proti DoS útokom

5.15 Pre organizácie so systémami alebo službami s vysokými nárokmi na dostupnosť je nutné zabezpečiť anti-DoS službu na strane poskytovateľa pripojenia do externej siete, ktorá zablokuje objemové DoS a DDoS útoky ešte pred vstupom do siete organizácie. Pre ostatné organizácie je takáto služba odporúčaná.

5.16 On-site by mala byť implementovaná anti-DoS ochrana chrániacia verejne dostupné služby aj proti ostatným typom DoS útokov ako sú zahltenie aplikácie, pomalé útoky ("low & slow") a SSL/TLS útoky. Takéto riešenie musí byť zabezpečené pre systémy a služby s vysokými nárokmi na dostupnosť (napr. právne záväzné elektronické služby občanom).

5.17 Anti-DoS riešenie musí notifikovať dedikovaný personál o výskyte prebiehajúceho útoku, alebo inej anomálie v sieťovej prevádzke. Anti-DoS riešenie musí logovať informácie o zablokovaných pokusoch o útok.

5.18 Odporúča sa implementovať vhodný rate-limiting na lokálnych a centrálnych FW.

Zabezpečenie DNS infraštruktúry

5.19 Autoritatívny DNS server by nemal byť zároveň rekurzívnym DNS serverom.

5.20 Autoritatívny DNS server musí povoľovať príjem požiadaviek na DNS Zone transfer len zo špecifikovaných IP adries a na Zóny, pre ktoré je autoritatívny. Musí povoľovať vykonať DNS transakciu "Zone transfer" len na špecifikované IP adresy.

5.21 Pre požiadavky aj odpovede na "Zone transfer" sa odporúča zabezpečiť autentifikáciu a integritu. Pre požiadavky aj odpovede na "Update" request by mala byť zabezpečená autentifikácia a integrita. Je možné podpisovať dopyty a odpovede zdieľaným kľúčom (využiť napr HMAC a RR TSIG). Pre každého klienta autoritatívneho servera by mal byť nakonfigurovaný iný kľúč.

5.22 Odporúča sa aby boli nakonfigurované ACL pre všetky typy DNS transakcií, ktoré povoľujú len požiadavky od špecifikovaných klientov.

5.23 DNS dopyty na name servery sa odporúča limitovať počtom z jednej IP adresy za špecifikovaný čas

5.24 Odpovede na DNS requesty by mali odchádzať z náhodného TCP/UDP portu

5.25 Odporúča sa aby autoritatívny a sekundárne DNS servery boli logicky a geograficky oddelené.

5.26 DNS záznamy o vnútorných zariadeniach nesmú byť prístupné z externch sietí (je možné využiť napríklad SPLIT DNS architektúru, alebo dve rôzne zóny).

5.27 Rekurzívny (cache) DNS server nesmie prijímať požiadavky z externých sietí. Nemal by byť z externých sietí vôbec prístupný.

5.28 Veľmi citlivé informácie nesmú byť uložené v rámci DNS (napr. špecifické HINFO alebo TXT záznamy)

5.29 DNS server by nemal zverejňovať informácie o použitom softvéri - minimálne nesmie odpovedať na špecifické dotazy typu "Version Query".

5.30 Musí byť rezervované doménové meno wpad.{doména}, kde {doména} je doménové meno používané v organizácii a publikované v odpovediach DHCP serverov. Rovnako pre všetky používané subdomény – t.j. wpad.{subdoména}.{doména}.

Zabezpečenie mailovej infraštruktúry

5.31 SMTP banner by nemal obsahovať informácie o použitom softvéri ani iné citlivé informácie. Nesmie byť možné zistiť verziu použitého softvéru prostredníctvom help príkazov.

5.32 Mailové správy odchádzajúce z organizácie by nemali obsahovať informácie o infraštruktúre organizácie (napríklad privátne IP adresy v hlavičke Received-From).

5.33 Odpoveď na príkaz VRFY by nemala obsahovať informáciu o existencií adresy alebo používateľského mena. Odporúča sa odpovedať kódom 252 s generickou hláškou.

5.34 Nemala by byť povolená metóda EXPN.

5.35 SMTP server by nemal preposlať e-mail, ktorý neobsahuje zdrojovú hlavičkovú e-mailovú adresu.

5.36 SMTP server musí prijímať správy na doručenie z externých sietí len pre spravované domény.

5.37 SMTP server musí prijímať správy na preposlanie len od autentifikovaných používateľov alebo z určených SMTP serverov.

5.38 Server by mal detegovať a blokovať pokusy o rozoslanie veľkého množstva e-mailov.

5.39 SMTP server musí kontrolovať správy pomocou anti-spam filtra.

5.40 SMTP server musí kontrolovať správy na prítomnosť škodlivého kódu

5.41 SMTP server musí logovať všetky detegované anomálie.

5.42 SMTP server musí logovať informácie o spracovávaných e-mailoch a tieto informácie by mali byť uchovávané aspoň 6 mesiacov. Musia byť uchovávané aspoň 3 mesiace.

5.43 Prístup k e-mailovým účtom musí byť možný len prostredníctvom šifrovaného kanála.

5.44 Odporúča sa na prístup k e-mailovej schránke nepoužívať proprietárne protokoly.

5.45 Z externých sietí by sa malo pristupovať na e-mail len prostredníctvom HTTPS alebo použitím štandardných protokolov POP3S alebo IMAPS. Odporúča sa autentifikovať klienta aj na základe certifikátu alebo vyžadovať použitie VPN. V prípade použitia iných protokolov by sa malo pristupovať prostredníctvom VPN pripojenia.

Zabezpečenie VPN infraštruktúry

5.46 Všetky VPN spojenia musia byť šifrované. Odporúča sa implementovať a vyžadovať šifrovanie spojenia s využitím Forward Secrecy.

5.47 Ak je potrebný vzdialený prístup k správcovským rozhraniam alebo do správcovskej siete, mala by byť využitá autentifikácia s využitím klientskych certifikátov. Aj pre bežných používateľov sa odporúča využiť autentifikáciu na základe klientskych certifikátov. Použité certifikáty musia používať aspoň RSA-2048, odporúča sa RSA-4096.

5.48 Ak sa používa PSK, musí byť použitý silný pre-shared key s entropiou aspoň 128 bitov. Odporúča sa náhodne generovaný reťazec.

5.49 VPN spojenia musia byť ukončované v samostatnom segmente.

5.50 Musia byť špecifikované FW pravidlá oddeľujúce sieť používateľov VPN a zvyšok internej siete a to metódou whitelistingu in aj out na princípe „least privilege“.

5.51 Ak sa používa SSL/TLS, mal by byť sa používaný len protokol TLS1.2. Nesmie byť použitý protokol SSL.

5.52 Nesmie byť možné vynegociovať použitie slabých šifier (ako sú napríklad sady šifier využívajúce RC4, DES a 3DES).

5.53 Na šifrovanie komunikácie by mal byť použitý protokol AES a to minimálne AES-128 (odporúča sa použiť AES-256). Pre prístup k citlivým IS alebo pre správcovskú VPN by mal byť na šifrovanie komunikácie použitý aspoň AES-256.

5.54 Mal by byť použitý hashovací algoritmus minimálne SHA-256

5.55 Ako algoritmus na výmenu kľúča by mal byť použitý DH (Diffie-Hellman) s dĺžkou aspoň 2048b.

5.56 Ďalšie požiadavky na zabezpečenie IPSec VPN:

a. VPN server nesmie umožniť využiť Aggresive mód nadviazania spojenia
b. Mal by sa používať len IKEv2
c. Platnosť šifrovacieho kľúča by mala byť nastavená na maximálne jeden deň
d. Odporúča sa skontrolovať politiky, ktoré sú k dispozícii pre IKE fázu 1 a odstániť politiky, ktoré umožňujú nastavenie málo bezpečných parametrov

5.57 Ďalšie požiadavky na zabezpečenie SSL VPN alebo Openvpn:

a. Klient musí overovať certifikát VPN servera
b. VPN server musí overovať platnosť klientskych certifikátov a mal by ju overovať aj voči CRL.
c. V klientskej konfigurácii OpenVPN sa odporúča používať perzistentné TUN/TAP rozhrania.

Zabezpečenie VOIP infraštruktúry a služieb videoconference

5.58 VOIP komunikácia z a do externých sietí by mala byť šifrovaná. Odporúča sa šifrovať aj internú VOIP komunikáciu (napr. SIP over TLS a SRTP a SRTCP).

5.59 VOIP zariadenia by mali byť z externých sietí do siete organizácie pripájané len cez VPN .

5.60 Všetky VOIP a telepresence zariadenia musia byť pred pripojením do siete hardenované (napr. podľa odporúčaní výrobcu).

5.61 Riadiaca komunikácia musí byť autentifikovaná (t.j. call signalling a web services signalling) a mala by byť aj šifrovaná.

5.62 Správcovské heslá telefónov musia byť komplexné a rôzne pre každé zariadenie.

5.63 Centrálny firewall by mal vedieť filtrovať VoIP komunikáciu. Odporúča sa nasadiť riešenie na filtrovanie VoIP spamu (SPIT - Spam over IP Telephony)

5.64 Pre konfiguračné súbory sťahované do telefónov by mala byť zabezpečená integrita a koncové zariadenia by mali overovať integritu týchto súborov.

5.65 Videoconferencing meeting by mal byť povinne šifrovaný (t.j. ak to zariadenie účastníka nepodporuje, nemôže sa zúčastniť).

5.66 Mal by byť použitý VOIP-aware firewall, ktorý umožňuje inšpekciu SIP protokolu.

5.67 SIP server musí byť na portoch TCP/UDP 5060/5061 dostupný len z potrebných zariadení.

5.68 Mal by byť použitý SBC (session border controller) a mal by ukončovať všetky prichádzajúce telefonáty a preposielať dáta cieľu (B2BUA)

5.69 Pohyblivá kamera na zariadení ako aj zapnutie mikrofónu nesmie byť ovládateľné na diaľku prostredníctvom siete.

5.70 Zariadenia pre videoconference by mali byť do siete pripájané len vtedy keď je to potrebné pre potreby videokonferencie alebo servisných zásahov.

5.71 Používané kamery, alebo zariadenia s kamerami, musia viditeľne indikovať, že sú zapnuté a snímajú.

Zabezpečenie iných služieb

5.72 Pre prístup k neštandardným službám, ktoré nie je možné hardenovať a zabezpečiť štandardným spôsobom (napr TLS) sa odporúča využiť prístup cez VPN.

Mechanizmus kontroly

5.73 Otvorené porty do Internetu by mali byť revidované aspoň raz za pol rok. Súčasťou revízie je sken otvorených portov do externých sietí a ohodnotenie, či sú naďalej potrebné.

5.74 Penetračné testy externej infraštruktúry by mali byť vykonané aspoň raz za rok.

5.75 Aspoň raz za rok by mali byť kontrolované verejne prístupné zdroje s cieľom skontrolovať, či nie sú zverejnené dôverné alebo citlivé informácie.

6 Minimálne požiadavky na zabezpečenie internej infraštruktúry

Implementácia architektúry riešenia

6.1 Sieť musí byť **segmentovaná na základe účelu** zariadení v jednotlivých segmentoch a rovnakých bezpečnostných požiadaviek. Minimálne takto:

a. Samostatné subsiete/VLAN pre oddelenia
b. Samostatné subsiete/VLAN pre manažment infraštruktúry a zálohovanie
c. Samostatné subsiete/VLAN pre manažment serverov a ich zálohovanie
d. Samostatné subsiete/VLAN pre servery s rovnakými bezpečnostnými požiadavkami
e. Samostatné subsiete/VLAN pre doménové radiče (okrem RODC)
f. Samostatné subsiete/VLAN pre manažment bezpečnostných prvkov
g. Samostatné subsiete/VLAN pre manažment virtualizačných serverov
h. Samostatné subsiete pre DMZ
i. Samostatné subsiete pre ICS/SCADA systémy
j. Samostatné subsiete pre VOIP
k. Samostatné subsiete pre wireless AP

6.2 Prepoje medzi jednotlivými segmentami sú chránené prostredníctvom ACL, ktoré sú nakonfigurované ne princípe „Least Privilege“.

6.3 Pre pripojenia pracovných staníc a všetky dostupné sieťové porty mimo zabezpečených priestorov by malo byť implementované Port Security, Dynamic ARP inspection a DHCP snooping. Ak sa používa IPv6, mali by byť implementované: NDP inspection a snooping, DHCPv6 snooping, RA Guard (Router Advertisement Guard).

6.4 Servery prístupné z externých sietí musia byť v iných segmentoch ako servery vnútornej infraštruktúry. Medzi týmito segmentami musí byť implementovaný firewall a ACL na princípe „Least Privilege“

6.5 V sieti by mal byť implementovaný OOBM (Out of band manažment).

6.6 Servery prístupné z externých sietí by mali byť na iných virtualizačných serveroch ako servery internej infraštruktúry

6.7 V sieti by mal byť implementovaný SSO (Single Sign-On) pre všetky systémy okrem kritických. Pre kritické systémy by mala vyžadovaná ďalšia úroveň autentifikácie prostredníctvom iného mena a hesla.

6.8 Pre prihlásenie do siete (do pracovnej stanice a na služby v doméne) odporúčame využívať dvojfaktorovú autentifikáciu.

6.9 V rámci implementácie architektúry by organizácia mala dodržiavať:

a. multi-vendor princíp pre bezpečnostné prvky
b. musí byť dodržané oddelenie DMZ, Perimetra (prvky, ktoré majú priamy prístup do Ineternetu) a interných častí siete.

c. VPN pripojenia musia byť ukončované v separátnych segmentoch a prístupy k ďalším častiam siete je možné iba prostredníctvom ACL na princípe „Least Privilege“.
d. Vnútorné servery ani pracovné stanice by nemali mať priamy prístup do Internetu ani externých sietí. Všetky pripojenia by mali prechádzať prostredníctvom perimetrových zariadení (Web a email proxy servery Proxy, aplikačné port forwardery pre potrebné iné služby)

6.10 V sieti by mali byť implementované lokálne NTP servery.

6.11 V sieti by mali byť implementované lokálne DNS servery.

6.12 V sieti by mali byť implementované lokálne Syslog servery.

6.13 V sieti by mali byť implementované lokálne update servery pre OS Windows aj Linux.

6.14 V sieti musia byť implementované:
a. Firewally na všetkých pripojeniach medzi sieťou organizácie a externými sieťami
b. Firewally na všetkých pripojeniach do kritických segmentov siete

6.15 V sieti by mali byť implementované:
a. IPS na všetkých pripojeniach medzi sieťou organizácie a externými sieťami
b. IPS/IDS na všetkých pripojeniach do kritických segmentov siete
c. Centralizované Anti malware riešenie na všetkých serveroch a pracovných staniciach.
d. Odporúčame ďalej implementovať sieťovú behaviorálnu analýzu na všetkých významných uzloch siete najmä však na známych perimetroch, prepojoch medzi DMZ, perimetrovými sieťami a vnútornou sieťou.

6.16 V infraštruktúre musia byť pravidelne aktualizované OS a všetky aplikácie a aspoň:
a. Raz za mesiac pre OS na platforme Windows
b. Raz za mesiac pre OS na platforme Linux a Unix
c. Raz denne pre antivírové riešenia na klientskych pracovných staniciach
d. Raz za týždeň pre antivírové riešenia na serveroch
e. Raz za 6 mesiacov pre OS bezpečnostných prvkov, sieťových prvkov a iných zariadení pripojených do infraštruktúry
f. Raz za mesiac všetky aplikácie na klientskych zariadeniach
g. Raz za rok všetky aplikácie a služby na serveroch

6.17 V infraštruktúre sa musia používať iba podporované verzie OS a aplikácií. Všetky výnimky musia byť schválené a implementované bezpečnostné opatrenia tak, aby nebolo možné tieto verzie zneužiť na kompromitáciu infraštruktúry.

6.18 Všetky účty, ktoré majú administrátorské oprávnenia musia spĺňať politiku hesiel pre účty s administrátorským prístupom.

6.19 Všetky účty, ktoré neboli použité do troch mesiacov (a zmenené heslo) od ich vytvorenia musia byť zablokované.

Hardening serverov, sieťových a bezpečnostných prvkov

6.20 Všetky nepoužívané a nepotrebné služby musia byť vypnuté.

6.21 Všetky firmware musia byť pravidelne aktualizované a hardenované podľa odporúčaní výrobcu.

6.22 Administračné rozhrania typu ILO resp. iDRAC musia byť aktualizované a prístupné iba z administrátorskej siete a musia byť v samostatných segmentoch.

6.23 Prístup k administrátorským rozhraniam musí byť iba zo siete administrátorov, ktorá je rozdielna od siete používateľov.

6.24 Servery nesmú umožniť prihlásenie anonymného používateľa (Guest prístup)

6.25 Servery musia mať nakonfigurovaný a udržiavaný host-based firewall (napríklad iptables v Linux alebo Windows firewall vo Windows) na princípe „least privilege“ pre spojenia dnu aj von.

6.26 Servery by mali mať partície na diskoch v RAID 1,5, 6, 10 alebo 50.

6.27 Všetky zariadenia by mali používať lokálne DNS servery.

6.28 Všetky zariadenia musia byť synchronizované s NTP serverom.

6.29 Všetky zariadenia by na synchronizáciu mali používať lokálny NTP server.

6.30 Všetky zariadenia by mali posielať logy na vzdialený logovací server:

a. Pre zariadenia ktoré podporujú syslog na vzdialený syslog server
b. Pre zariadenia Windows na vzdialený Windows Log server prostredníctvom funkcionality Windows Event Forwarding

6.31 Všetky servery by mali mať nainštalované antimalware riešenie s centrálnym manažmenotom a zberom logov .

6.32 Syslog servery:

a. Musia mať dostupnú dostatočnú diskovú kapacitu na uloženie dát aspoň na 6 mesiacov
b. Musia byť synchronizované s NTP serverom
c. Logy musia byť pravidelne zálohované (minimálne raz za mesiac)
d. Logy musia byť pre všetkých používateľov syslog serveru nastavené ibana čítanie

6.33 Administračné rozhrania by mali byť prístupné iba prostredníctvom šifrovaných sieťových kanálov.

a. Šifrované kanály sa musia prezentovať dôveryhodným verejným kľúčom alebo certifikátom
b. V prípade, že nie je možné používať šifrované kanály by malo byť implementované ACL na princípe "Least privilege" a vyčlenené tieto rozhrania do samostatných segmentov

6.34 Logovanie musí zaznamenávať[15]:

15 Ak to uvedená technológia umožňuje

a. (Úspešné aj neúspešné) Prihlásenie a odhlásenie
b. (Úspešné aj neúspešné) Spustenie procesu alebo služby
c. (Úspešné aj neúspešné) Vytvorenie, modifikáciu alebo zmazanie používateľa alebo skupiny
d. (Úspešné aj neúspešné) Pokusy pristúpiť k citlivým údajom (údaje klasifikované hornými dvomi klasifikačnými stupňami v rámci organizácie)
e. (Úspešné aj neúspešné) Spustenie a ukončenie procesu
f. (Úspešné aj neúspešné) Prihlásenie sa zo systému na iný systém alebo službu

Sieťové prvky

6.35 Všetky nepotrebné služby musia byť vypnuté alebo odinštalované.

6.36 OS/firmvéry by mali byť pravidelne aktualizované.

6.37 Používateľské heslá by nemali byť uložené v reverzibilnom formáte.

6.38 Mala by byť implementovaná centrálna SSO (Single sign-on) autentifikácia prostredníctvom protokolov Radius, Tacacs+ alebo Diameter.

6.39 Pre pripojenie pracovných staníc by mala organizácia využívať NAC (napríklad NAP alebo 802.1x).

6.40 Vo všetkých manažmentových segmentoch by mala byť implementovaná PVLAN.

6.41 Vo všetkých používateľských segmentoch by mala byť implementovaná PVLAN.

Monitoring

6.42 V sieti by mal byť implementovaný dohľad nad funkčnosťou zariadení a služieb.

6.43 V rámci siete by mal byť implementovaný bezpečnostný monitoring ktorý bude monitorovať aspoň:
a. Bezpečnostné prvky
b. Sieťové prvky v organizácií
c. Doménu Windows

6.44 V sieti by nemalo byť používané SNMPv2 a malo by byť používané SNMPv3.
a. V prípade použitia SNMPv2 musia community reťazce spĺňať politiku hesiel pre účty s administrátorským prístupom.
b. Community reťazce musia byť unikátne pre sieťový segment a účel použitia

6.45 Pre všetky dátové toky a služby v rámci monitoringu musia byť implementované ACL na princípe "Least privilege".

Tlačiarne

6.46 Tlačiarne by mali byť umiestnené v samostatnom segmente.

6.47 Správcovské rozhrania by mali byť prístupné iba z administrátorskej siete a musí byť na správcovskom rozhraní implementovaná autentifikácia a účty musia spĺňať politiku hesiel pre používateľov.

6.48 Tlačiarne by mali byť prístupné klientom iba prostredníctvom tlačových serverov.

Windows infraštruktúra

6.49 Na všetkých serveroch musí byť zakázaný prístup na čítanie prostredníctvom neautentifikovaného používateľa (napríklad ošetrená tzv. CIFS null zraniteľnosť)

6.50 Na doménových kontroleroch nesmú byť ukladané heslá prostredníctvom Group Policy Preferences v aplikovaných doménových politikách.

6.51 Všetky interné servery by mali byť v doméne.

6.52 Autentifikácia na servery by mala byť iba prostredníctvom Kerberosu

6.53 Autentifikácia prostredníctvom NTLM by mala byť zakázaná

6.54 SMB podpisovanie musí byť vyžadované

6.55 Na všetkých serveroch musia byť implementované dôveryhodné certifikáty na prístup ku všetkým službám (RDP, HTTPS,LDAPS,..)

6.56 Doménoví administrátori a enterprise administrátori musia mať zakázaný prístup a autentifikáciu na všetky pracovné stanice.

6.57 Servery prístupné z externých sietí nie sú v doméne alebo sa autentifikujú voči RODC, ktorý je v samostatnom segmente (DMZ) a je prístupný iba z ostatných DMZ.

6.58 Administrátorské a používateľské účty administrátorov musia byť oddelené a mať rozdielne heslá

6.59 Doménoví administrátori by mali využívať dvojfaktorovú autentifikáciu

6.60 Počítače musia byť do domény pridávané pod samostatným účtom, ktorý ma oprávnenie iba pridávať počítače do domény. Žiadni iní používatelia nesmú mať právo pridať počítač do domény.

6.61 V sieti by malo byť vypnuté prostredníctvom GPO automatické vyhľadávanie proxy servera WPAD. Konfigurácia proxy servera by mala byť nakonfigurovaná prostredníctvom GPO.

6.62 Implementácia nového softvéru na servery by mala prebiehať prostredníctvom balíčkovacích nástrojov (Deployment services resp. System center)

6.63 Remote powershell execution by malo byť povolené len z administrátorskej siete.

6.64 V prípade používania RDP musí byť možné prihlasovanie iba v restricted režime (RDP restricted admin).

6.65 GPO preferences musia byť vypnuté

Mechanizmus kontroly

6.66 Mal by byť interný penetračný test aspoň raz za 2 roky. Aplikovanie odporúčaní výsledkov penetračného testu.

6.67 Odporúča sa vykonať interný technický audit splnenia požiadaviek plynúcich z tohto dokumentu.

7 Minimálne požiadavky na zabezpečenie pracovných staníc pristupujúcich k implementovanému riešeniu

Všeobecné požiadavky

7.1 Na pracovných staniciach musí byť nainštalované anti-malware riešenie
   a. Riešenie musí byť pravidelne aktualizované (aspoň jeden krát za deň)
   b. Riešenie musí byť pravidelne využité na skenovanie pracovnej stanice (aspoň raz za týždeň)
   c. Riešenie musí podporovať rezidentnú ochranu[16] a táto musí byť aktívna
   d. Riešenie by malo byť centrálne spravované a malo by mať centrálne vyhodnocované výsledky skenov a detekcie hrozieb
   e. Logy z anti-malware riešenia musia byť archivované minimálne 6 mesiacov

7.2 OS, všetky jeho súčasti a nainštalované aplikácie musia byť vo verziách podporovaných výrobcom a pravidelne aktualizované (najviac s oneskorením jeden mesiac).

7.3 Aktualizácie a mitigácie pre kritické zraniteľnosti (s vysokým dopadom) by mali byť aplikované do 72 hodín od ich zverejnenia na pracovných staniciach, z ktorých je možný prístup ku kritickým systémom a dátam. Mal by byť vedený zoznam takýchto staníc.

7.4 Na pracovných staniciach by malo byť zapnuté automatické sťahovanie a inštalácia aktualizácií.

7.5 Na pracovných staniciach musí byť implementovaný lokálny firewall:
   a. Všetky prichádzajúce aj odchádzajúce spojenia musia byť zakázané okrem spojení, ktoré sú potrebné na štandardnú činnosť aplikácie.
   b. Pravidlá vo firewalli by mali byť centrálne spravované a implementované na princípe „least privilege“
   c. Všetky zakázané spojenia musia byť archivované minimálne na dobu 6 mesiacov.
   d. Informácie o zakázaných spojenia by mali byť archivované na centrálnom úložisku

Logovanie

7.6 Bezpečnostné Logy z pracovných staníc by mali byť odosielané na centrálny server a ukladané minimálne po dobu 6 mesiacov.

7.7 Na pracovných staniciach by malo byť logovanie nastavené minimálne v rozsahu:
   a. (Úspešné aj neúspešné) Prihlásenie a odhlásenie
   b. (Úspešné aj neúspešné) Spustenie procesu alebo služby
   c. (Úspešné aj neúspešné) Vytvorenie, modifikáciu alebo zmazanie používateľa alebo skupiny
   d. (Úspešné aj neúspešné) Pokusy o prihlásenie prostredníctvom RDP, SSH

Hardening

7.8 Pracovná stanica musí byť hardenovaná minimálne v rozsahu
   a. Všetky Windows pracovné stanice musia byť pripojené do domény

16 t.j. detekciu škodlivého kódu pri otváraní súborov a spúšťaní programov

b. Všetky služby, ktoré nie sú potrebné sú odinštalované alebo aspoň zakázané alebo vypnuté.
c. Všetky programy a súčasti OS, ktoré nie sú potrebné sú odinštalované
d. Všetky programy boli povolené a otestované bezpečnostným útvarom organizácie
e. Používatelia nemajú administrátorské oprávnenia
f. Lokálne administrátorské účty sú neaktívne. Ak musia byť z nejakého dôvodu aktívne heslá k týmto účtom spĺňajú požiadavky na heslá pre účty s administrátorským prístupom[17]
g. Pracovné stanice musia na prihlásenie vyžadovať heslo
h. Po dobe nečiinosti (najviac 30 minút) musí byť spustený šetrič obrazovky a uzamknutá pracovná plocha

7.9 V prípade pracovných staníc s OS Windows musí byť pracovná stanica hardenovaná minimálne v rozsahu:
a. Používatelia nemajú právo inštalácie softvéru
b. Používatelia ani administrátori nemajú oprávnenie Debug procesu
c. Na pracovnej stanici je počet uložených hashov prihlasovacích účtov nastavený na maximálne dva[18].
d. Na pracovnej stanici by mal byť implementovaný whitelisting spúšťateľných súborov (napr. Applocker alebo Software Restriction Policies [SRP]) tak, aby bolo možné spúšťať iba dôveryhodné povolené aplikácie.
e. Na pracovnej stanici musí byť zapnutý UAC (User Access Control) a mal by byť nastavený na najvyššiu hodnotu.
f. Na pracovnej stanici by mal byť nainštalovaný a nakonfigurovaný nástroj EMET (od Microsoft) so zapnutými všetkými ochranami, ktoré je možné zapnúť. Ak pre niektorý používaný program nie je možné zapnúť všetky ochrany, odporúča sa prehodnotiť potrebu jeho používania.
g. Doménový administrátori a ostatní privilegovaní používatelia nemajú oprávnenie na prihlásenie sa na pracovné stanice.
h. Na pracovnej stanici je vypnuté automatické spúšťanie programov po vložení vymeniteľného média (Autoplay)
i. IPv6 by malo byť vypnuté, pokiaľ nie je používané
j. NetBios nad IPv4 by mal byť vypnutý
k. Makrá v MS Office by mali byť vypnuté a nemalo by byť možné ich povoliť. Ak sú makrá používané, malo by byť ich vykonávanie povolené len pre konkrétneho používateľa a len z dôveryhodných špecifikovaných lokalít (nie z Internetu), prípadne implementovať podpisovanie makier pomocou PKI.
l. Lokálne účty nesmú byť zlinkované s MICROSOFT ID
m. Dáta na pracovnej stanici nesmú byť synchronizované prostredníctvom verejných služieb (OneDrive, DROPBox, google drive, MEga a podobne)

7.10 Prenosné pracovné stanice musia byť hardenované minimálne v rozsahu:

17 Viď prílohu Politika hesiel
18 kľúč registra HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows_NT\ CurrentVersion\Winlogon\ CachedLogonsCount

a. Disk musí byť šifrovaný (Full disk encryption)
b. Záložný kľúč k šifrovanému disku by mala mať organizácia k dispozícií (Implementovaný key escrow mechanizmus)
c. BIOS/UEFI by mal byť chránený heslom pri prenosných zariadeniach.

7.11 Webové prehliadače by mali mať implementovanú funkcionalitu alebo rozšírenia:
a. Rozšírenie na blokovanie spúšťania skriptov (napr. NoScript)
b. Rozšírenie na blokovanie reklamy (napr. Adblock, UBlock Origin)
c. Rozšírenie na blokovanie trackerov (napr. Privacy Badger)

Mechanizmus kontroly

Rovnaký ako pre internú infraštruktúru.

8 Administratívne opatrenia

Všeobecné požiadavky

8.1 V organizácii musí byť vytvorená, vedením schválená, implementovaná, dokumentovaná a dodržiavaná Bezpečnostná politika, ktorá spĺňa aspoň nasledovné požiadavky:

a. Je adekvátna veľkosti, typu, zameraniu a činnostiam organizácie.
b. Definuje bezpečnostné ciele, spôsob ich schvaľovania, dosahovania a merania účinnosti ich dosahovania.
c. Vyjadruje záväzok vedenia organizácie dosahovať stanovené bezpečnostné ciele a spĺňať požiadavky všetkých zainteresovaných strán.
d. Definuje rozsah a pravidelnosť školení zamestnancov a iných aktivít zameraných na zvyšovanie povedomia o informačnej bezpečnosti, súvisiacich hrozbách a možnostiach ochrany pred týmito hrozbami.
e. Je publikovaná na mieste prístupnom všetkým zamestnancom a je propagovaná v rámci organizácie a v rámci školení – a to aspoň každých 12 mesiacov – je adekvátne komunikovaná všetkým zamestnancom.
f. Definuje roly a zodpovednosti za informačnú bezpečnosť. Musia byť definované zodpovednosti aspoň pre tieto roly: vrcholný predstaviteľ organizácie, manažér pre bezpečnosť, vedúci pracovník, administrátor, audítor, používateľ.
g. Definuje spôsob riadenia informačných aktív a spôsob vedenia inventáru/zoznamu týchto aktív.
h. Definuje spôsob vykonávania manažmentu rizík informačnej bezpečnosti.
i. Definuje spôsob nahlasovania a reakcie na bezpečnostné incidenty.
j. Definuje spôsob vykonávania a frekvenciu preskúmavania bezpečnostnej politiky.
k. Definuje spôsob vykonávania a frekvenciu vykonávania interných auditov informačnej bezpečnosti.

8.2 V organizácii musí byť vytvorená, vedením schválená, implementovaná, dokumentovaná a dodržiavaná Smernica pre manažment rizík informačnej bezpečnosti, ktorá spĺňa aspoň nasledovné požiadavky:

a. Definuje spôsob identifikácie a ohodnotenia informačných aktív.
b. Definuje spôsob identifikácie a ohodnotenia hrozieb, ktoré vplývajú na informačné aktíva.
c. Definuje spôsob identifikácie a ohodnotenia zraniteľností, ktoré informačné aktíva obsahujú.
d. Definuje spôsob ohodnotenia rizík na základe identifikovaných hrozieb a zraniteľností.
e. Definuje postup pre výber spôsobu ošetrenia identifikovaných rizík (napr. redukcia rizika, akceptácia rizika, vyhnutie sa riziku, resp. prenos rizika na inú stranu).
f. Definuje spôsob pre vytvorenie Plánu pre ošetrenie rizík, ktorý stanovuje konkrétne opatrenia, zodpovednosti za implementáciu týchto opatrení, termíny a potrebné zdroje na ošetrenie rizík.
g. Definuje spôsob vyhodnotenia efektívnosti implementovaných opatrení.

8.3 V organizácii musí byť vytvorená, vedením schválená, implementovaná, dokumentovaná a dodržiavaná Smernica pre bezpečné používanie aktív, ktorá spĺňa aspoň nasledovné požiadavky:

a. Definuje pravidlá pre bezpečné používanie e-mailu, služieb v Internete a iných komunikačných prostriedkov.
b. Definuje pravidlá pre bezpečnú prácu s heslami.
c. Definuje pravidlá pre inštaláciu hardvéru a softvéru.
d. Stanovuje zákaz inštalácie alebo používania neautorizovaného alebo nelegálneho softvéru.
e. Definuje pravidlá pre ochranu pred škodlivým softvérom a základnými útokmi na používateľa.
f. Definuje pravidlá pre bezpečné používanie aktív mimo priestorov organizácie.
g. Je publikovaná na mieste prístupnom všetkým zamestnancom a je propagovaná v rámci organizácie a v rámci školení – a to aspoň každých 12 mesiacov – je adekvátne komunikovaná všetkým zamestnancom.
h. Je pravidelne preskúmavaná aspoň každých 12 mesiacov a v prípade zmien v organizácii alebo zmien v jej IS alebo v prípade výskytu bezpečnostných incidentov je aktualizovaná a jej zmena je komunikovaná všetkým zamestnancom organizácie.

8.4 V organizácii musí byť vytvorená, vedením schválená, implementovaná, dokumentovaná a dodržiavaná Smernica pre riadenie prístupu, ktorá spĺňa aspoň nasledovné požiadavky:

a. Definuje spôsob žiadania o prístup, schvaľovania a prideľovania prístupu k jednotlivým IS v organizácii a fyzickým priestorom na základe objektívnej potreby a zamýšľaného používania IS či potreby prístupu do fyzických priestorov.
b. Definuje zodpovednosti za prideľovanie, monitorovanie, pravidelné preskúmavanie prístupových práv do IS a odstraňovanie neplatných účtov.
c. Definuje spôsob monitorovania prístupov do IS, monitorovania používania IS a vyhodnocovania auditných log záznamov.
d. Definuje spôsob riadenia jednotlivých typov prístupových účtov a manažment privilégií.
e. Definuje spôsob implementácie oddelenia povinností (Separation of Duties) s cieľom predchádzať škodlivej aktivite a chybám.
f. Definuje spôsob implementácie minimálnych privilégií (Least Privilege) s cieľom zaistiť prístup len k tým aktívam, IS a aplikáciám, ktoré sú potrebné na vykonávanie pracovných úloh.
g. Definuje spôsob časového obmedzenia používania aktív, IS a aplikácií a spôsob uzamknutia relácie pri definovanom čase nečinnosti používateľa.
h. Definuje spôsob vzdialeného prístupu k aktívam, IS a aplikáciám, monitorovanie vzdialeného prístupu a bezpečnostné požiadavky pre vzdialený prístup.
i. Definuje spôsob riadenia prístupu k bezdrôtovým sieťam.
j. Definuje spôsob riadenia prístupu mobilných zariadení.
k. Definuje spôsob riadenia prístupu k IS organizácie s verejne dostupným obsahom (napr. webové sídlo, účet na sociálnych sieťach a pod.).

8.5 V organizácii musí byť vytvorená, vedením schválená, implementovaná, dokumentovaná a dodržiavaná Smernica pre riešenie počítačových bezpečnostných incidentov, ktorá spĺňa

aspoň nasledovné požiadavky:

a. Definuje spôsob klasifikácie incidentov, ktorý obsahuje aspoň nasledovné typy incidentov: nežiaduci obsah, škodlivý kód, získavanie informácií, pokus o prienik, prienik, nedostupnosť, ohrozenie bezpečnosti informácií, podvod, sprenevera.
b. Definuje spôsob komunikácie, komunikačné kanály a postupy nahlasovania incidentov.
c. Definuje roly a zodpovednosti pri riešení incidentov.
d. Definuje spôsob riešenia incidentov.
e. Definuje spôsob zaistenia dôkazov.
f. Definuje spôsob vedenia dokumentácie o bezpečnostných incidentoch.
g. Definuje spôsob vyšetrovania bezpečnostných incidentov, spôsob vyvodzovania zodpovednosti a ukladaní sankcií za spôsobený incident.

8.6 V organizácii musí byť vytvorená, vedením schválená, implementovaná, dokumentovaná a dodržiavaná Smernica pre riadenie kontinuity činností, ktorá spĺňa aspoň nasledovné požiadavky:

a. Definuje roly a zodpovednosti za jednotlivé činnosti pri riadení kontinuity činností.
b. Definuje ciele riadenia kontinuity činností.
c. Definuje požiadavky na vykonanie analýzy dopadov a analýzy rizík.
d. Definuje spôsob určenia cieľovej doby obnovy (RTO – recovery time objective) a cieľového bodu obnovy (RPO – recovery point objective) pre jednotlivé procesy, IS a aplikácie.
e. Definuje spôsob tvorenia stratégie kontinuity činností.
f. Definuje spôsob vytvorenia havarijných plánov a plánov obnovy.
g. Definuje komunikačné plány v prípade mimoriadnej udalosti (prerušenia činností).
h. Definuje frekvenciu vykonávania cvičení a testovania plánov kontinuity činností a školení.
i. Definuje frekvenciu preskúmavania a aktualizácie plánov kontinuity činností.

8.7 Zmluvy s dodávateľmi musia ustanoviť právo organizácie vykonať u dodávateľa audit bezpečnosti informačných systémov a kontrolu dodržiavania bezpečnostných požiadaviek. Taktiež musia zaväzovať dodávateľa opraviť prípadné nájdené nedostatky.

8.8 Organizácia musí, pri dodávaní služieb súvisiacich s IKT, s dodávateľom uzavrieť dohodu o úrovni poskytovania služieb (SLA), ktorá musí obsahovať aspoň[19]:

a. Bezpečnostné opatrenia, ktoré je dodávateľ povinný dodržiavať.
b. Požiadavky na monitorovanie súladu s SLA a aktívne hlásenie nedodržania bezpečnostných požiadaviek a bezpečnostných incidentov súvisiacich s poskytovaním služieb.
c. Dohodu, že aktivity vykonávané dodávateľom sú ním dokumentované a podliehajú kontrole a auditu zo strany organizácie.
d. Finančné pokuty za nedodržanie dohody.
e. Právo na odstúpenie od dohody v prípade, že nie sú naplnené jej podmienky.

8.9 V organizácii musia byť zavedené nasledovné predpisy:

a. Bezpečnostná politika pre prácu tretích strán a ich účasť v procesoch organizácie.

19 Template SLA (časť informačná bezpečnosť) je dostupný na webstránkach https://www.csirt.sk.

b. Smernica pre vzdialený prístup do IS organizácie.
c. Smernica pre zálohovanie.
d. Smernica pre klasifikáciu informácií.

8.10 V organizácii by mali byť zavedené nasledovné predpisy:
a. Smernica pre výkon interného auditu.
b. Smernica pre BYOD a prácu na diaľku.
c. Smernica pre ničenie informácií a ich nosičov.
d. Smernica pre riadenie zmien.
e. Smernica pre riadenie zraniteľností a implementáciu záplat.

8.11 V organizácii musia byť vedené aspoň nasledovné záznamy:
a. Záznamy o školeniach, kvalifikácii a skúsenostiach zamestnancov.
b. Výsledky monitorovania a merania informačnej bezpečnosti.
c. Program interných auditov a výsledky (správy) z vykonania interných auditov.
d. Log záznamy, záznamy o bezpečnostných udalostiach a bezpečnostných incidentoch.

Mechanizmus kontroly

8.12 Bezpečnostná politika a bezpečnostné smernice musia byť pravidelne preskúmavané manažérom bezpečnosti aspoň raz za každých 12 mesiacov a vždy v prípade zmien v organizácii alebo v jej informačných systémoch, alebo v prípade výskytu bezpečnostných incidentov.

8.13 Dodržiavanie bezpečnostnej politiky a bezpečnostných smerníc musí byť pravidelne kontrolované prostredníctvom pravidelných interných auditov informačnej bezpečnosti.

Príloha A – Politika hesiel

Heslá pre účty s administrátorskými oprávneniami

- Dĺžka hesla musí byť aspoň 14 znakov
- Heslá musia obsahovať
    - aspoň jedno veľké písmeno
    - aspoň jedno malé písmeno
    - aspoň jednu číslicu
    - aspoň jeden špeciálny znak
- Odporúčame aby heslo obsahovalo
    - aspoň jeden znak s diakritikou (ak je heslo používané v rámci homogénneho prostredia)
- Zmena hesla
    - Odporúča sa aby heslá boli menené aspoň raz za 3 mesiace
    - Heslá by mali byť zmenené aspoň raz za rok
    - Odporúča sa aby zmenené heslá mali od pôvodného hesla editačnú vzdialenosť aspoň 7 (t.j. počet operácií vymazania, vloženia alebo prepísania znaku, ktorými sa z pôvodného hesla dá získať nové)
    - Zmenené heslo by nemalo byť jedným z posledných 24 hesiel v histórii hesiel pre daný účet
    - Heslo je možné zmeniť najviac raz za 1 deň.

Heslá pre účty s privilegovaným prístupom

- Dĺžka hesla musí byť aspoň 12 znakov (20 znakov pre systémové a technické účty)
- Heslá musia obsahovať
    - aspoň jedno veľké písmeno
    - aspoň jedno malé písmeno
    - aspoň jednu číslicu
    - aspoň jeden špeciálny znak
- Zmena hesla
    - Heslá by mali byť menené aspoň raz za 3 mesiace
    - Heslá musia byť zmenené aspoň raz za 2 roky
    - Zmenené heslá musia mať zmenené viac ako polovicu znakov oproti pôvodnému heslu
    - Zmenené heslo nesmie byť jedným z posledných 24 hesiel v histórii hesiel pre daný účet

Heslá pre neprivilegované účty

- Dĺžka hesla musí byť aspoň 12 znakov
- Heslá musia obsahovať
    - aspoň jedno veľké písmeno

    - aspoň jedno malé písmeno
    - aspoň jednu číslicu
    - aspoň jeden špeciálny znak
- Zmena hesla
    - Heslá by mali byť menené aspoň raz za 6 mesiacov
    - Heslá musia byť zmenené aspoň raz za rok
    - Zmenené heslo nesmie byť jedným z posledných 12 hesiel v histórii hesiel pre daný účet
    - Heslo je možné zmeniť najviac raz za 1 deň.

Príloha B - Zariadenia pre nasadenie a zabezpečenie webového servera

Je dostupných mnoho typov bezpečnostných zariadení, určených na zabezpečenie webových serverov. Vyššie uvedené bezpečnostné odporúčania možno do istej miery implementovať pomocou nich. Tieto zariadenia umocňujú účinok opatrení. Môžu zabrániť v prístupe útočníka k webovému serveru, čo je výhodné najmä počas doby odstraňovania novozisteného bezpečnostného nedostatku.

Medzi najznámejšie funkcie zariadení určených na zabezpečenie webového servera patria:

- SSL akcelerátory – preberajú náročné výpočty potrebné na nadviazanie SSL/TLS spojení
- Bezpečnostné brány – monitorujú HTTP prevádzku v smere do a od webového servera, v prípade podozrenia na útok vykonajú opatrenia podľa potreby
- Content filtre – monitorujú prevádzku webového servera v oboch smeroch, po stránke obsahovej: v prípade zaznamenania citlivých či nevhodných dát podľa potreby vykonajú opatrenia
- Autentifikačné brány – rôznymi mechanizmami autentifikujú používateľov, riadia prístup k URL na webovom serveri

V mnohých prípadoch sú vyššie uvedené funkcie kombinované v jedinom zariadení, často označovanom ako reverzné proxy.

Na zjednodušenie a zvýšenie bezpečnosti už pri prvotnej inštalácií webového servera možno použiť niektoré spomedzi balíčkov, kombinujúcich hardenovaný operačný systém a webový server. Spravidla ide o zabezpečený univerzálny OS (Linux, Windows, ...) prispôsobený na podporu bezpečne konfigurovaného webového servera (Apache, IIS, ...). Podobné riešenia sa opierajú o

- Bezpečnú defaultnú konfiguráciu
- Hardenovaný OS/TOS
- Hardenovaný software webového servera
- Rozšírené možnosti auditu
- Aplikačné wrappery
- Sieťové wrappery a/alebo funkcia host-based firewallu
- Host-based IDS

- Zjednodušená administrácia bezpečnosti (napr. GUI či menu)

Webaplikačné firewally (WAF) sú špeciálnym typom firewallu, prispôsobeným na zabezpečenie webového servera. Ide o filter, plugin či zariadenie ktorý aplikuje set pravidiel na HTTP prevádzku. Všeobecne tieto pravidlá pokrývajú útoky ako XSS a SQL Injection. Prispôsobením potrebám aplikácie môže byť pomocou WAF množstvo útokov eliminovaných. WAF sa pôvodne zameriavali na monitorovanie prevádzky na aplikačnej vrstve, teda na úrovni HTTP protokolu. V súčasnosti sa funkcie tradičného WAF kombinujú s inými robustnými sieťovými technológiami, ako sú load balancing, sieťové firewally či aplikačné servery.

K bezpečnosti webových služieb môžu výrazne prispieť prvky použité na zabezpečenie externej infraštruktúry, ako firewally či IDS/IPS riešenia. Venuje sa im nasledujúca kapitola tohto dokumentu.

Nasadenie HW a SW zariadení na zvýšenie ochrany webového servera možno odporúčať. Konfigurácia zariadenia však musí zodpovedať požiadavkám na zabezpečenie konkrétneho servera a musí byť v súlade s opatreniami, uvedenými vyššie v tejto kapitole. Pri použití predpripravených balíčkov OS s webovým serverom je potrebné preveriť súlad východzej konfigurácie s popísanými požiadavkami a podľa potreby nastavenia upraviť. Kontrola továrenských nastavení a konfigurácia podľa definovaných požiadaviek je potrebná pri akomkoľvek spomínanom bezpečnostnom riešení.

Pozn. V tomto dokumente sa nevenujeme problematike tzv. web appliances, teda zariadení špeciálne určených iba na beh webového servera. Ide o zariadenia so zjednodušeným operačným systémom a s množinou služieb nutnou na beh webového servera. Optimalizovaný OS a minimum nadbytočných servisov, konfiguračných možností a jednoduchá správa z týchto zariadení robí riešenie vhodné pre malé až stredné aplikácie. Cieľom dokumentu je však poskytnúť komplexné odporúčania, vhodné i pre zložité, viacvrstvové modely webových aplikácií, pre ktorých funkciu jednoduché jednoúčelové zariadenie nepostačuje.