NEXTECH

KYBERNETICKÁ BEZPEČNOSŤ

PRE FIRMY 2023

PREVENCIA
Ako sa pripraviť a priebežne kontrolovať stav ochrany

OCHRANA
Aké útoky hrozia firmám a ako sa pred nimi chrániť

REAKCIA
Čo robiť ak už k útoku došlo, ako reagovať

OBSAH:

TECHNOLÓGIE

Druhy kybernetických útokov 6
Finančný sektor býva cieľom kybernetických útokov 300× častejšie ako iné firmy 10
S únikom dát sa stretli až dve tretiny malých a stredných firiem 12
Audit kybernetickej bezpečnosti 14
Havarijný plán, reakcie na incidenty, postup obnovenia fungovania IT 19
Analýza hrozieb, potenciálnych rizík a identifikácia zraniteľných miest 20
Inventarizácia softvéru 22
Správa a zabezpečenie koncových zariadení 23
Zabezpečenie mobilných zariadení 27
Posúdenie kybernetických hrozieb program CTAP 31
Technické vynútenie dodržiavania bezpečnostných politík 32
Využívanie vlastných zariadení na pracovné účely (BYOD) 34

PROCESY

Motivácia na zabezpečenie IT systémov 36
Manažérstvo informačnej bezpečnosti, bezpečnostný plán 38
Manažér kybernetickej bezpečnosti: požiadavky kladené na výkon funkcie 41
Koncový používateľ ako prvý krok kybernetickej bezpečnosti 42
Vzdelávanie zamestnancov 44
Clashing: Zvýšte povedomie zamestnancov o kybernetickej bezpečnosti 46
Ako predísť pomste zamestnancov 48
Ochrana údajov 50
Zabezpečenie sietí 52
Bezpečnosť v cloude 56

LEGISLATÍVA

Prehľad zákonov a vyhlášok 59
Bezpečnostná IT politika vo firme 60
Dodržiavanie bezpečnostných politík 65
Ochrana osobných údajov 66
Zoznam partnerov 70

KYBERNETICKÁ BEZPEČNOSŤ PRE FIRMY 2023

VYDÁVA:
Digital Visions, s. r. o.
Kladnianska 60, 821 05 Bratislava
e-mail: info@nextech.sk,
http: www.nextech.sk

VÝKONNÝ RIADITEĽ:
Martin Drobný

ODBORNÝ REDAKTOR:
Ľuboslav Lacko

ASISTENT VYDANIA, INZERCIA:
Ľudmila Gebauerová

GRAFIKA:
Peter Mačuga

Za obsah inzerátov zodpovedajú inzerenti.
Ďalšia reprodukcia článkov možná len so súhlasom vydavateľa.
Tlač: z dodaných reprodukčných materiálov.
Zdroj foto strana 1: rawpixel.com on Freepik.

ISBN 978-80-974206-6-6

CYBERGAME 2023

Kyberbezpečnostná hra pre študentov, talentovaných hráčov, programátorov aj profesionálov rôznej úrovne

15 scenárov
70+ úloh

Výhry v kategóriách

- Najlepší hráč
- Najlepšia hráčka
- Hráči vo vetvách
- Študent
- Najmladší hráč
- Učitelia
- Zamestnanci verejnej správy

- MALVÉROVÁ ANALÝZA
- HARDENING
- PROCESY A RIADENIE BEZPEČNOSTI
- OSINT
- FORENZNÁ ANALÝZA
- KRYPTOGRAFIA

Nominácia a tréning národného tímu na European Cyber Security Challenge 2023

Tréningová platforma pre organizácie
01/10/2023 – 31/10/2023

ODBORNÁ GARANCIA
SK CERT
NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

www.cybergame.sk
01/03/2023 – 10/05/2023

ALITER TECHNOLOGIES · CHECK POINT · REPUBLIC OF GAMERS · IBM · ALISON · eset Digital Security Progress. Protected. · Microsoft · elkan smart learning · BCH BUKOVINSKÝ & CHLÁPALA · VEEAM · Kompetenčné a certifikačné centrum kybernetickej bezpečnosti · rtvs: Rozhlas a televízia Slovenska · ZIVE

THIS IS NOT A GAME, THIS IS CYBERGAME

TECHNICKÉ VYNÚTENIE DODRŽIAVANIA BEZPEČNOSTNÝCH POLITÍK

Nie je žiadna novinka, že pri životnom cykle bezpečnostných politík musíme brať do úvahy všetky aspekty a prostriedky, ktoré budú s touto politikou späté – technické prostriedky, procesy a ľudí. Všetky tieto aspekty a prostriedky musíme zohľadňovať už pri návrhu bezpečnostnej politiky. Navyše to, čo veľkou mierou determinuje ako sa bude bezpečnostná politika dodržiavať, je jej správna definícia s ohľadom na legislatívne a bezpečnostné praktiky a hlavne jej správna definícia vzhľadom na ciele organizácie. Aj tá najlepšia bezpečnostná politika sa bude obchádzať, resp. jej dodržiavanie bude technicky veľmi náročné, ak nebude v súlade s cieľmi organizácie. V ideálnom prípade by mala bezpečnostná politika tieto ciele podporovať.

Technické opatrenia hrajú prím

Nielen ľudská hlúposť a vesmír, ako by povedal slávny fyzik 20. storočia Albert Einstein, ale aj ľudská vynaliezavosť je nekonečná. Na tento fakt by sme mali myslieť zakaždým, keď zvažujeme, aké technické, procesné či ľudské aspekty bude treba použiť pri vynucovaní bezpečnostnej politiky. Keby navyše bezpečnostná politika nepodporovala incentívy jej používateľov či nesledovala ciele spoločnosti, dostali by sme takmer „dokonalú" kombináciu, v ktorej bude extrémne náročné zabezpečiť vynucovanie akejkoľvek bezpečnostnej politiky.

Technologické opatrenia hrajú prím. Na dosiahnutie optimálnych výsledkov pri vynucovaní bezpečnostných politík je dôležité primárne sa sústrediť na technické opatrenia. V ideálnom prípade by nastavenie technológií malo reflektovať nastavenie bezpečnostnej politiky a minimalizovať tak priestor na svojvoľné správanie používateľov. Hoci môže takéto tvrdenie znieť príliš represívne, musíme si uvedomiť, že ak nastavenie technológie nasleduje ciele spoločnosti a motivačné faktory používateľov, potom dostávame ideálny model, kde sú používatelia motivovaní dodržiavať bezpečnostné pravidlá, no zároveň vychádzame z najlepších bezpečnostných odporúčaní, kde je presne definované, čo a ako používatelia môžu vykonávať, pričom všetko ostatné je zakázané. Samozrejmou výhodou pri používaní technických prostriedkov je, že ich môžeme považovať za deterministické (ak odhliadneme od náhodných a softvé-

rových problémov) v porovnaní s ľudským správaním, ich správanie sa nemení a nie je náchylné na náhodné chyby. Použitie technologických prostriedkov vieme veľkou mierou automatizovať a takisto modulárnosť takéhoto prístupu je oveľa väčšia.

Moderné bezpečnostné nástroje využívajúce metódy behaviorálnej analýzy či umelej inteligencie nám zároveň pomáhajú tieto politiky, resp. technické prostriedky nastaviť oveľa dynamickejšie. Bezpečnostné politiky môžu byť oveľa granulárnejšie, môžeme v nich zohľadniť kontext používateľa, ako aj jeho správanie a podľa toho prideliť represívnejšiu či voľnejšiu politiku.

Myšlienku môžeme ilustrovať na politike hesiel, ako verím, každému čitateľovi veľmi dobre známej. O dôležitosti dobre zvolených a komplexných hesiel nemusíme polemizovať, poďme sa však pozrieť na dva spôsoby, ako vynútiť takúto politiku bezpečného hesla.

Klasický spôsob: Technickými prostriedkami nastavíme vynucovane veľmi silného hesla. Hoci je toto nastavenie technicky v poriadku, pri veľmi komplexnom hesle skončíme ľahko v stave, keď nemalá časť používateľov začne túto politiku obchádzať – heslá na papierikoch pod klávesnicou či na monitore by neboli prekvapujúce. V takomto prípade technicky správne nastavená politika priniesla ku koncu dňa zníženie informačnej bezpečnosti.

Vyvážený spôsob: Technickými prostriedkami nastavíme vynucovanie menej komplexného hesla. Toto heslo bude použité pri prihlasovaní v rámci lokálnej LAN, keď sa vykonalo overenie PC alebo sa realizovala behaviorálna analýza používateľa a jeho kontextu (ako a kedy sa prihlásil, ako rýchlo sa prihlásil, pohyby myšou...). Pri pripojení z VPN, prípadne ak kontext nebude potvrdený, budeme vyžadovať potvrdenie cez druhý faktor, napr. potvrdením push notifikácie na mobile či iného HW prvku.

Samozrejme, použitie vyváženého spôsobu prináša použitie pokročilých technologických opatrení, no zároveň veľmi efektívne vynucuje bezpečnostnú politiku prihlásenia, pričom používatelia nie sú motivovaní na jej obchádzanie. Takýmto nastavením by sme docielili zvýšenie úrovne informačnej bezpečnosti s ohľadom na motiváciu používateľov – jednoduché prihlásenie do informačných systémov.

Záver

Hoci technologické prostriedky hrajú pri uvažovaní o ideálnom nastavení bezpečnostnej politiky prím, bolo by naivné si myslieť, že samotné nastavenie týchto technologických prostriedkov je dostačujúce. Domnievam sa, že aj v tomto prípade by sme vedeli vhodne aplikovať Paretov princíp, keď väčšinu ťarchy presunieme na bedrá technológie, no zďaleka nehovoríme o celej ťarche. Správna definícia interných procesov či pravidelné vzdelávanie a zvyšovanie povedomia v oblasti informačnej bezpečnosti ostáva naďalej veľmi dôležitou súčasťou všetkých bezpečnostných politík. Aj v ideálnom prípade musíme nad technológiou udržiavať procesy, ako sú pravidelné aktualizácie či skúmanie logovacích záznamov na overenie funkčnosti a auditných záznamov.

V každej organizácii nastanú situácie, keď napriek tomu, že vhodná technológia existuje, z objektívnych dôvod nemôže byť použitá. V takomto prípade musíme využiť dostupnú technológiu a dodržiavanie bezpečnostných pravidiel ošetriť napr. dodatočnými kontrolnými procesmi či zvýšenou aktivitou v oblasti vzdelávania používateľov.

Vynucovanie bezpečnostných politík predstavuje neustále balansovanie medzi tým, aké technické opatrenia, aké procesy či vzdelávacie aktivity použiť. Navyše tento balans musí zohľadňovať aj faktory, ako sú súlad s legislatívou a v neposlednom rade súlad so smerovaním organizácie.

MICHAL **SRNEC**, CISO ALITER TECHNOLOGIES

ÚVODNÝ OBRÁZOK **FREEPIK ON FREEPIK.COM**

Za obsah a inšpiráciu k tejto téme ďakujeme

www.aliter.com

ALITER TECHNOLOGIES