N°01 - 2022
technická příloha
K-net Technical International Group

Vaše téma

NOVINKY BEZPEČNOSTNÍCH ŘEŠENÍ V IT

Bezpečnost v IT je stále obrovské téma. Množství útoků se neustále zvyšuje a útoky jsou sofistikovanější a lépe zpracované. Za poslední rok jsme zaznamenali nespočet útoků na naše datové centrum, ale i u našich zákazníků. Musím říci, že rozdíly oproti útokům v minulosti jsou obrovské. Jednak jejich počet dramaticky stoupá, ale i jejich provedení je na úplně jiné úrovni. Myslet si, já jsem malá firma nebo organizace, na mě nikdo útočit nebude, je už absolutně chybná myšlenka.

Útočníka už vůbec nezajímá velikost organizace ani citlivost jejich dat. Pokud zjistí jen sebemenší díru či možnost zaútočit, tak to vyzkouší. A je pouze na dané organizaci, jak je připravena útokům odolat. Také představa, že investuji do drahých bezpečnostních technologií, je mylná. Útoky jsou aktuálně směřované spíše na lidi (konkrétní zaměstnance). Proto je potřeba IT bezpečnost pojmout komplexně a zaměřit se nejen na technologie, ale i na vzdělanost zaměstnanců, kvalitní monitoring a dohled. V této příloze Loginu se podíváme nejen na technologické novinky pro řešení IT bezpečnosti na perimetru sítě, ale také si řekneme, co znamená penetrační testování zaměřené na koncové uživatele.

Ing. Petr Nepustil
vedoucí divize Výroba

OBSAH TECHNICKÉ PŘÍLOHY:

AKTUALITY

Nové vlastnosti Forcepoint DLP

Útočníci aktuálně cílí na získávání nejen kontaktů konkrétního uživatele, ale také získávání přesných textů e-mailů, aby následně mohli zaútočit na konkrétního uživatele s velmi věrohodným textem, získat jeho důvěru a následně provést útok například podvrženou fakturou s platbou na účet útočníka. S novým vydáním Forcepoint DLP 8.9 mohou zákazníci efektivněji chránit data opouštějící e-maily, získat větší viditelnost a kontrolu nad aplikacemi Microsoft (Office) 365 a zlepšit automatizaci a kontrolu dat z populárních nástrojů ITSM a BI.
Nově i pro odchozí cloudový email Forcepoint poskytuje více než 1 500 předdefinovaných šablon a klasifikátorů využívajících automatizaci, strojové učení a otisky prstů, což umožňuje velmi přesné zásady pro identifikaci dat a souborů na základě kterých dojde k pozastavení odeslání. Mohou existovat data, která budou vyžadovat zvláštní pozornost v Teams, a nebudou potřebovat stejný typ pozornosti (a akce) v SharePointu. Forcepoint teď nabízí možnost implementovat různé akce s různým chováním, a tedy různou granularitu zabezpečení v Teams, SharePointu a OneDrivu.
Správa incidentů DLP je nyní možná přes rozhraní REST API aplikacemi třetích stran. V první vlně se jedná o služby ServiceNow, Nagios a Tableau.

Forcepoint je dceřiná společnost americké společnosti Raytheon, největšího výrobce špičkové vojenské techniky. Bezpečnost je jejich priorita číslo 1. Zaměřuje se nejen na řešení NGF firewallů, ale také na ochranu před únikem informací (DLP – Data Lost Prevention), tedy řešení pro předcházení ztráty dat.

Nová úroveň ochrany v českém kyberprostoru

V současné době pozorujeme jednoznačný trend uzavírat veškerou komunikaci do šifrovaných kanálů. Dříve běžně používané nešifrované protokoly, jako je HTTP, SMTP nebo DNS, jsou vytlačovány svými šifrovanými variantami (jako například TLS verze 1.3 nebo HTTP/3), které velmi znesnadňují nebo přímo znemožňují jejich kontrolu. Éra, kdy administrátor na perimetru sítí prováděl inspekci provozu, pomalu končí.

Na současnou situaci reaguje **KERNUN ADAPTIVE FIREWALL**. Jeho bezpečnostní komponenta „Adaptivní firewall" využívá metadata spojená s komunikací (SRC IP, DST IP, počty spojení atd.) a srovnává je s informacemi uloženými v aktuální databázi hrozeb. Dojde-li k identifikaci útočníka, je pokus o útok na všech zařízeních zablokován.

Expertní databáze hrozeb je tvořena a spravována bezpečnostním týmem KERNUN CSIRT, který úzce spolupracuje s národními bezpečnostními autoritami a CSIRT týmy komerčních firem i státní správy. Právě šíře zapojení a plošné nasazení služby na mnoha zařízeních umožňuje správné vyhodnocení informací o potencionálním útočníkovi a přináší radikální zvýšení bezpečnosti pro české internetové prostředí, které je aplikováno ihned.

PŘÍKLAD VYHODNOCENÍ KYBERNETICKÉHO ÚTOKU ADAPTIVNÍM FIREWALLEM SKRZE DATABÁZI AKTIVNÍCH HROZEB

Představte si několik krátkých SSH spojení z jedné adresy na druhou, která proběhla v rámci krátkého časového úseku. Je to útok nebo není? Může jít o útočné pokusy uhodnout heslo, anebo o legitimní zkopírování několika menších souborů. Standardní IPS/IDS systém to může buď odmítnout nebo povolit, anebo ohlásit jako varování. V každém z těchto případů jde o riziko vzniku false-positive nebo false-negative, případně systém nechá rozhodnutí na člověku a vytvoří pouze varování.
Oproti tomu může mít Kernun Adaptive Firewall navíc informaci, že se tato adresa pokusila provést obdobná SSH spojení také na tisíce jiných adres. V takovém případě ji považuje za útočnou a spojení nepovolí už při prvním pokusu. Adresa má tzv. špatnou reputaci (důvěryhodnost). Naopak absence jakéhokoliv podezřelého chování zdrojové adresy ve sledovaných sítích českého internetu ukazuje, že adresa bude s vysokou pravděpodobností neškodná.
Situace se může ale rychle změnit. Pokud se začnou z této adresy objevovat spojení pochybná, její reputace se rapidně sníží a další spojení s ní už nebudou povolena. Jestliže tedy v českém internetu probíhá nějaký cílený kybernetický útok, adaptivní firewall se o něm záhy dozví a může rychle a efektivně reagovat přímo v místě svého nasazení. Chrání tak konkrétní cíle právě tady a teď.
Z výše uvedeného je zřejmé, že pro rozhodnutí o tom, kdo je nebo může být útočník, je potřeba aktivně sledovat a hodnotit širší síťový kontext.

+

Zajímají vás možnosti zlepšení kybernetické bezpečnosti ve vaší organizaci?
Chcete zjistit, jestli by Kernun Adaptive Firewall odhalil nebezpečný provoz, který vaší sítí může běžně procházet? Kontaktujte nás, společně připravíme nejlepší řešení

k.k-net.cz/technologie-kernun

PENETRAČNÍ TESTOVÁNÍ

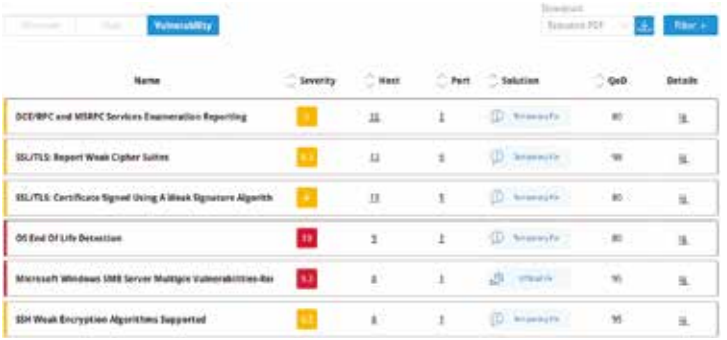
Co je penetrační testování

Pojem penetrační testování je velice rozšířený, ale ne každý si pod ním představí stejnou věc.
Dle Wikipedie: *„Penetrační test je v informatice metoda hodnocení zabezpečení počítačových zařízení, systémů nebo aplikací. Provádí se testováním, simulací možných útoků na tento systém jak zevnitř, tak zvenčí. Cílem penetračního testu není vyřešit bezpečnostní problémy, ale jistým způsobem prověřit, zhodnotit úroveň zabezpečení a podat souhrnnou zprávu, a to jak na úrovni technických (nastavení otevřených portů, verze systému), tak i organizačních opatření (podvod a sociální inženýrství skrze zaměstnance)“.*
Britské Národní centrum pro kybernetickou bezpečnost popisuje penetrační testování jako: *„Metoda pro získání jistoty v bezpečnosti IT systému pokusem o narušení části nebo celé bezpečnosti tohoto systému pomocí stejných nástrojů a technik, jaké by mohl mít protivník.“*

Důležité je si uvědomit, že v rámci penetračního testování se opravdu jedná o různé druhy testů a prověřování bezpečnostních děr, a to nejen na straně bezpečnostních technologií, ale i na straně uživatelů. Komplexní penetrační test tedy není jednoduchá ani levná záležitost, protože je vykonáván přímo bezpečnostními specialisty a testování a vyhodnocování zabere jednotky až desítky dní. Pro management může být penetrační testování nástrojem pro ověření stavu kybernetické odolnosti. Ta se týká schopnosti subjektu nepřetržitě dosahovat zamýšleného výsledku navzdory nepříznivým kybernetickým událostem. Je reakcí na zvyšující se počty útoků a rizik spojených se sociálním inženýrstvím a zneužitím uživatelů a zabývá se nikoliv pouze prevencí, ale snížením dopadu samotného útoku a rychlostí obnovení činnosti po útoku v plném rozsahu.
Penetrační testování je možné rozdělit podle dvou hlavních oblastí – **technologické** a **organizační**. Pro technologické testování můžeme využívat i automatizované služby.

Bezpečnostní test IT technologií na základě známých zranitelností

Pro základní představu o zabezpečení IT technologií počítačové sítě provádíme penetrační test s využitím automatizace.
K-net využívá pro testování vlastního datového centra stejně jako pro testování IT technologií zákazníků služby s využitím databáze „Greenbone Enterprise Feed“. Jedná se o řešení, které pracuje s více než 100.000 zranitelnostmi, ke kterým má připravené programy s konkrétními bezpečnostními testy a je neustále rozšiřováno (příklad zranitelnosti s vysvětlením jejího popisu je uveden dále).
Testování může probíhat ze strany internetu nebo z vnitřní sítě a ověřit tak, jestli technologie nemá nějaké známé bezpečnostní díry či chybná nastavení.



Tabulka zjištěných zranitelností

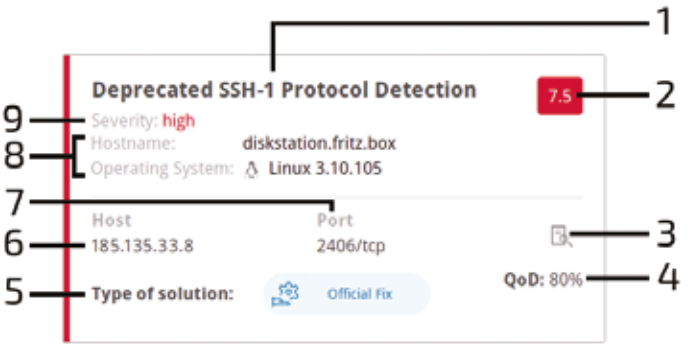
Výsledky testování jsou připraveny ve formě dvou reportů:

1. **Pro management**, který obsahuje obecné informace o kontrole a seznamy hostitelů seřazené podle závažnosti zjištění.
2. **Pro techniky**, který obsahuje rovněž obecné informace o kontrole a o kontrolovaných hostitelích, ale také podrobnosti o každé nalezené zranitelnosti.

Významné události jsou potom komentovány včetně návrhu jejich řešení našimi specialisty.
Tento bezpečnostní test nemusí být cenově náročný, protože díky cloudovým technologiím je možné ho realizovat jednorázově na vybraných IP adresách.

VÝSLEDEK SKENOVÁNÍ – DETAIL ZRANITELNOSTI

U každého výsledku se zobrazí následující informace:



Ukázka zápisu zranitelnosti

1. Název nalezené zranitelnosti.
2. Závažnost zranitelnosti.
3. Otevřete překryvnou vrstvu s podrobnostmi o zranitelnosti.
4. QoD je zkratka pro „Quality of Detection" a ukazuje spolehlivost detekce zranitelnosti.
5. Typ řešení pro nalezenou chybu zabezpečení. Jsou možná následující řešení:
   a. Oficiální oprava: je k dispozici oprava oficiálního dodavatele. Pokud není uvedeno jinak, předpokládá se, že tato oprava tuto chybu zabezpečení plně řeší.
   b. Dočasná oprava: k dočasnému odstranění této chyby zabezpečení je k dispozici náhradní řešení; náhradní řešení může být jedno, více nebo také zatím nemusí existovat.
   c. Snížení rizika: jsou k dispozici informace o konfiguraci nebo scénáři nasazení, které pomáhají snížit riziko zranitelnosti, ale neřeší zranitelnost dotčeného produktu.
   d. ... další možnosti (neexistuje a nebude, hledání opravy atd.).
6. Hostitel, pro kterého byl nalezen výsledek.
7. Číslo portu a typ protokolu použitý k nalezení zranitelnosti hostitele.
8. Název hostitele a operační systém hostitele, pro kterého byl nalezen výsledek.
9. Úroveň závažnosti zranitelnosti.

Komplexní penetrační testování

Cílem penetračního testování je komplexně zhodnotit síťovou infrastrukturu, informační systém nebo webovou aplikaci vůči jak z pohledu útočníků na internetu, tak i třeba z řad zlomyslných zaměstnanců.
Zahrnuje v sobě několik disciplín a je určitě výbornou součástí pro projekty spojené se zvýšením kybernetické bezpečnosti, s nasazením ISO 27001, dosažením souladu s GDPR či jinými bezpečnostními normami, nebo projektem zabývajícím se zajištěním provozu organizace, a tedy i její kybernetické odolnosti, možná také připravujete školení a chcete znát, na co se u svých uživatelů zaměřit.
Z hlediska projektu sledujeme dvě linie Organizační (co všechno potřebujeme k testování) a Technickou (členění na testované oblasti).
Vše, co je zde uvedeno můžeme také využít pro intenzivní test pouze některé části nebo komponenty vaší informatiky.

JAK POSTUPUJEME (ORGANIZACE PROJEKTU)

Penetrační testování vyžaduje systematický přístup. Pro dosažení vysoké kvality a informační hodnoty výsledků je nezbytné zvolit správný postup. Ten zahrnuje sběr informací, hodnocení aktiv a identifikaci cílů, identifikaci zranitelností, verifikaci zranitelností a pokus o narušení bezpečnosti, identifikaci dopadů a jejich odstranění po zneužití zranitelností, tvorbu závěrečné zprávy a závěrečný re-test.

CO TESTUJEME (PENETRAČNÍ TESTY PODLE OBLASTÍ)

PENETRAČNÍ TESTY IT INFRASTRUKTURY

Interní penetrační test
V průběhu testu je simulován pokus o průnik z pozice útočníka, který získal přístup k interní síti. Jedním z cílů je také zneužití testovaných systémů k vlastním škodlivým aktivitám.

Externí penetrační test
V průběhu testu je simulován pokus o průnik anonymního útočníka z internetové sítě, který se snaží o průnik do interní sítě, případně o získání citlivých dat. Hlavním cílem je získání přístupu do interní sítě klienta.

PENETRAČNÍ TESTY WEBOVÝCH A MOBILNÍCH APLIKACÍ

Cílem penetračního testu aplikace a souvisejících služeb je nestandardními akcemi uživatele demonstrovat zranitelnosti, kterými je možno realizovat průnik do interní infrastruktury nebo získat citlivá data či upozornit na chyby v aplikační logice.

PENETRAČNÍ TESTY ODOLNOSTI UŽIVATELŮ

Penetrační testy odolnosti uživatelů využívají metod sociálního inženýrství a jsou zaměřeny na praktické testování uživatelů a jejich povědomí o informační bezpečnosti. Cílem je testování samotných uživatelů za účelem získání citlivých informací, dat a zdrojů.

E-mailový test – Phishing
Cílem testování je prověřit úroveň bezpečnostního povědomí uživatelů a přimět je sdělit citlivé informace nebo vykonat nebezpečnou akci. Scénáře budou přizpůsobeny požadavkům zákazníka a mohou obsahovat i škodlivý balíček simulující malware, webový portál apod.

Telefonický test – Vishing
Podkladem testu jsou telefonní čísla veřejně dostupná na internetu, sdělená zadavatelem nebo přímo získaná samotným testerem. Na tato čísla jsou pak vedeny podvodné telefonické hovory.

Cílený test – Spear phishing
Spear phishing představuje cílený phishingový útok na předem vytipované osoby (vrcholové manažery nebo doménové administrátory). Test je rozšířen o podrobnou analýzu cíle, aby byl přesně zacílený na daného představitele.

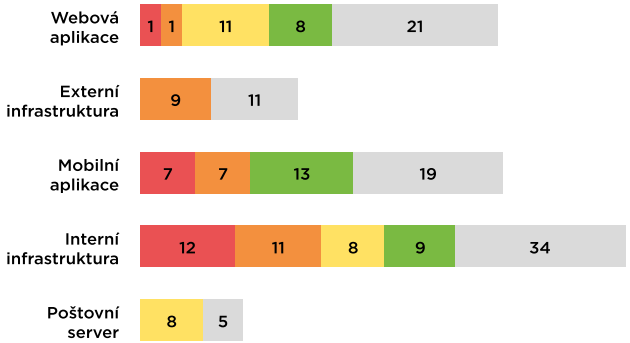
Aktivní test fyzické bezpečnosti
Základem testu je pokus o fyzický průnik neautorizované osoby do vnitřních prostor organizace, které jsou v běžném režimu veřejnosti nepřístupné.

Pasivní test fyzické bezpečnosti
V rámci testu jsou ve vybraných lokalitách umístěny USB flash disky s potenciálně nebezpečným obsahem. Cílem testu je sledovat a vyhodnotit chování uživatelů.

VÝSTUP TESTOVÁNÍ

Přináší strategické informace a přehled o slabých místech využitelných k průniku do testovaných systémů. Definuje stupeň jejich závažnosti a navrhuje nápravná opatření k jejich eliminaci. Nalezené bezpečnostní nedostatky a zranitelnosti jsou klasifikovány pomocí pětibodové stupnice, která zachycuje úroveň rizika: informativní / nízká / střední / vysoká / kritická dle metodiky CVSS. V případě zjištění kritické nebo vysoké zranitelnosti v průběhu penetračního testování jsou tato zjištění sdělována odpovědným osobám zadavatele bezodkladně.

Komplexní penetrační testování vyžaduje tým zkušených bezpečnostních specialistů, kteří testy provádějí. K-net a jeho IT specialisté spolupracují na testování s odborným týmem etických hackerů.



Kritické
Možnost ovládnutí domény
Zranitelnost HP Protector umožňující spuštění kódu
Slabá hesla doménových účtů

Vysoké
Únik citlivých informací skrze dostupné síťové disky
Nedostatky v zabezpečení SSH
Zneužití multicast protokolů

Střední
Přístupný git repozitář
Náchylnost aplikace k DoS
Podpora služby Telnet

Nízké
Informační únik privátní adresy MS Exchange

Informativní
Neplatný reverzní záznam DNS

Příklad klasifikace ve výstupní zprávě

ZAUJALO VÁS TÉMA TECHNICKÉ PŘÍLOHY?

Přečtěte si její nezkrácenou verzi na našem webu s doplňujícími informacemi na

k.k-net.cz/tp-bezpecnostni-reseni

K-net Technical International Group, s.r.o.
Olomoucká 170
627 00 Brno – Černovice
tel.: 548 220 150
GSM: 734 686 001
Pobočka: Rovečínská 16
679 74 Olešnice
tel.: 511 447 055

K-net Team Praha, s.r.o.
Sazečská 560/8
108 00 Praha 10 – Malešice
tel.: 734 686 014

K-net Team Ostrava, s.r.o.
Smetanovo náměstí 328/1
702 00 Ostrava
tel.: 734 686 012

facebook.k-net.cz
linkedin.k-net.cz
youtube.k-net.cz
info@k-net.cz

www.k-net.cz

Vysvětlení podtržených výrazů z Loginu a Technické přílohy najdete v glosáři IT pojmů na **k.k-net.cz/glosar**

Technická příloha časopisu LOGIN 1/2022, ročník č. 17 | *Připravili: Marie Hamerská, Věra Staňková, Jana Hejtmánková, Jan Crlík, Tomáš Knettig, Petr Nepustil*
Poděkování za přípravu podkladů patří firmám Kernum a TNS.
Vydala společnost K-net | Neprodejné | Uzávěrka čísla: 8. 5. 2022