NetSHIELD řešení pro GDPR

Narušení bezpečnosti je stále aktuální téma, které je veřejností, v médiích i na odborných diskuzích ostře sledováno. Z hlediska našich zkušeností a znalostí cítíme naléhavou potřebu posunout do centra pozornosti posílení IT bezpečnosti. Cybersecurity Ventures dokonce předpovídá, že kyber-kriminalita a její následky budou stát do roku 2021 podniky $ 6 bilionů ročně. Obecné požadavky nařízení EU o ochraně osobních údajů (GDPR), jsou již zdokumentovány, vymahatelné a žalovatelné. Vše proto, aby pomohly organizacím při zavádění preventivních opatření jako reakci na současnou kybernetickou situaci ve světě.

Až Nařízení o obecné ochraně údajů (GDPR) vstoupí v platnost dne 25. května 2018, všechny společnosti mající osobní data jednotlivců nacházející se v členských státech EU musí být v souladu s tímto právním ustanovením. GDPR postihuje každou společnost, která zpracovává osobní údaje občanů EU, ať už na náklady, nebo zdarma. Porušení klíčových ustanovení GDPR může mít za následek pokuty až do výše 4 % globálního celosvětového ročního obratu podniku v předchozím finančním roce.

GDPR nás oficiálně utvrzuje v tom, jak důležité je soukromí spotřebitelů a jak vážný přestupek je jeho porušení. GDPR stanovuje rámec dodržování pravidel, na nichž lze stavět bezpečnostní infrastrukturu schopnou poskytovat odpovídající ochranu osobních údajů. Bohužel z průzkumu společnosti Dell z roku 2016 vyplývá, že 97 % firem nemá vypracován žádný plán počítající s dodržováním GDPR.

Je třeba vzít v úvahu, že ani jediný dodavatel momentálně není schopen dodávat komplexní řešení pro GDPR, nicméně je třeba zvážit množství faktorů. Ačkoli jsou všichni povinni být připraveni v květnu 2018, je dobré se začít připravovat již nyní a hloubková síťová kontrola je výborným výchozím bodem. NetSHIELD jako takový využívá výhod více než deseti let dodávaného bezpečnostního řešení a bude konkrétně řešit dva klíčové body uvedené v GDPR.

GDPR řešení od NetSHIELDu se konkrétně zabývá články 32 a 37 nařízení EU o ochraně osobních údajů. Ty definují systémovou integritu sítě a zvyšují povědomí o ochraně osobních údajů. Bohužel tyto nařízení jsou zatím chudé na detaily. Nicméně je nezbytné, aby byly firmy připraveny. NetSHIELD usnadňuje organizacím nasazení řešení pro analýzu rizik, zajištění trvalé integrity sítě a nabízí jedinečné řešení schopné zajistit dodržování GDPR.

Bod 32 požaduje, aby organizace „Zajistila důvěrnost, integritu, dostupnost, a odolnost systému“. Klíčovým problémem je, že jen velmi málo organizací dnes provozuje „důvěryhodnou LAN“. Firmy neprovozující “důvěryhodnou LAN” nemohou zajistit důvěrnost, integritu, dostupnost a odolnost sítě. IT bylo v průběhu posledních pěti let značně zatíženo novými technologiemi, které sice přinášejí efektivnost a úsporu času, ale často bohužel na úkor síťové bezpečnosti.

- Díky virtualizaci bylo možné téměř okamžitě spustit VM (Virtual Machine). Problém spočívá v tom, že VM se poměrně hodně rozšiřuje, což znamená, že některé z těchto VM jsou stále aktivní, i když se například nevyužívají a zůstávají nespravované po několik měsíců.
- BYOD a rozvoj podnikové mobility znemožnily IT udržet krok s bezpečnostními požadavky a kontrolou těchto zařízení. Zabezpečení mobilních zařízení je často opomíjeno a je převážně řízeno pouze minimálním bezpečnostním požadavky, které poskytuje sdílené Wi-Fi připojení.
- Nyní jsme na vrcholu trendu internetu věcí. Společnost Cisco předpovídá, že v příštích 3-5 letech se k síti připojí 50 až 200 miliard nových zařízení. Tato zařízení nejsou schopna přijímat zabezpečení založené na agentu a jako taková představují významnou bezpečnostní výzvu pro dnešní bezpečnost.

Můžete zajistit systémovou "integritu" bez úplného povědomí o všech zařízeních, které se připojují k síti? NetSHIELD tuto viditelnost poskytuje. Navíc poskytuje správcům IT možnost odhalovat a řídit všechna propojená zařízení, stejně jako schopnost dynamicky blokovat neznámé nebo nedůvěryhodné zařízení. Řešení „NetSHIELD“ umožňuje

organizacím snadné nasazení řešení pro analýzu síťových rizik, získání okamžité kontroly firemních sítí LAN a zajištění trvalé integrity sítě.

Bod 37 požaduje, aby organizace poskytovaly "Zvyšování povědomí a školení zaměstnanců zapojených do zpracování operací/informací". Obecně platí, že toto je dodáváno v rámci tréninkového procesu, který je často žalostně nedostatečný při přípravě zaměstnanců tak, aby identifikovali a úspěšně omezili pokročilý útok malware.

NetSHIELD nabízí unikátní opěrné body, které jsou mimořádně přínosné, aby zajistil vysoce efektivní a rozšířenou průběžnou odbornou přípravu. Malware se stále vyvíjí a je neustále inovován tak, že se zaměřuje na jeden z nejzranitelnějších vstupních bodů organizace – samotné zaměstnance. Bohužel se až příliš často stávají obětí některých z pokročilých a dobře skrytých útoků. Zpráva o vyšetřování narušení bezpečnosti osobních údajů společnosti Verizon naznačuje, že bylo otevřeno 30 % zpráv o phishingu – od zprávy za rok 2015 to je nárůst o 23 %. 13 % z těch, kteří klikli, otevřeli škodlivou přílohu nebo špatný odkaz.

Rámec tréninku „NetSHIELD GDPR Training Awareness Solution“ zahrnuje:

- Dynamickou blokaci malware, phishing a ransomware před napadením firemních koncových bodů. IT oddělení je okamžitě upozorněno na tyto blokované pokusy.
- Upozornění může být dodáváno také HR, aby se výrazně zvýšila úspěšnost školení, poskytnutím vzorků z praxe. Neexistuje vhodnější způsob, aby byli zaměstnanci vybaveni znalostmi o detekci malware.
- Skutečné příklady pro zvýraznění vyspělosti a sofistikovanosti škodlivého malware/phishingu.
- Významné zvyšování povědomí zaměstnanců tak, aby se mohli účinně zapojit do boje proti škodlivému malware.

NetSHIELD je pokročilé řešení postavené na rámci více než desetiletí pokročilých řešení kyber-bezpečnosti. NetSHIELD je dobře propojen se změnami, které přináší GDPR, stejně jako s průmyslovými standardy, jako je britský Cyber Essentials Assurance Framework a National Institute of Standards and Technology’s (NIST). Je navržen tak, aby sloužil firmám všech velikostí a úrovní.

Řešení NetSHIELD GDPR poskytuje organizacím možnost analýzy rizik, sestavení plánu pro zlepšení, zajištění integrity sítě a nabízí opěrné body tréninku, což jsou důležité body pro splnění požadavků GDPR.

GDPR bude mít mnohem větší dopad na ostatní národy mimo EU. EU a USA již vyjednávají o ochraně soukromí. Tento nový a jednotnější přístup však bude vyžadovat, aby organizace upravily svou současnou strategii ochrany údajů a upřednostňovaly zavedení příslušné bezpečnostní infrastruktury a kontrol.

Vzhledem k dnešnímu hyperaktivnímu kybernetickému prostředí je kriticky důležité, aby organizace myslely jinak. Příliš často organizace pokračují v investicích do oblastí, které se stávají méně efektivní, neboť aktéři malwaru čelí již řadu let typickému vzorci bezpečnostní infrastruktury. Je zřejmé, že firewall, antivir a podobně nejsou dostatečné pro řešení všech zranitelností zabezpečení organizace. Níže uvádíme přesvědčivou matici definovanou institutem SANS, která ilustruje výdaje na bezpečnost. Kontrola přístupu do sítě je definována jako velmi důležitá a je často oblastí, která je přehlížena mnoha organizacemi.

"Důvěryhodná síť LAN" je příliš často přehlížena i když je to kritická oblast pro zabezpečení. Vzhledem k šíření nových zařízení a typů zařízení, které se připojily k sítím za posledních pět let, včetně virtuálních koncových bodů, zařízení BYOD a zařízení IoT, byla schopnost IT identifikovat a řídit tuto infrastrukturu výrazně snížena. Je zřejmé, že je třeba obnovit "důvěryhodnou síť LAN".

7 klíčových úvah, které by organizace měly vzít v úvahu, aby zajistily komplexní bezpečnost a připravily se na požadavky GDPR a Privacy Shield:

1. Pokračujte v tom, co již bylo označeno za normativní, neboť bezpečnost je kritickým obchodním imperativem. Zálohování, šifrování, firewally, antiviry atd. Jedná se o efektivní komponenty, které však nejsou dostatečné pro řešení všech zranitelností organizací. V roce 2016 organizace investovaly téměř 100 milionů dolarů do zabezpečení. Bohužel počítačová kriminalita z loňského roku vyčerpala 600 miliard dolarů z globální ekonomiky. Očekává se, že do roku 2021 se toto číslo zvýší na 6 bilionů dolarů. Je vaše prognóza růstu 10-ti násobkem, aby udržovala krok s touto negativní prognózou výnosů?

   Předpokládá se, že škody na počítačovou kriminalitu se do roku 2021 vyšplhají na 6 bilionu dolarů. – CSO, IDG

2. Začněte myslet o bezpečnosti jinak, protože kriminální živly dávno vědí, co děláte. Začněte s kritickou bezpečností zevnitř ven.

   Průměrný počet dnů, po kterém Útočníci zůstávají v síti před detekcí, je více než 200 - Microsoft Advanced Threat Analytics | Microsoft

3. Obnovte důvěryhodnou síť LAN. Mějte přehled a řídte, kdo a co se k vám připojuje prostřednictvím fyzických, virtuálních, mobilních a IoT zařízení. To o čem nevíte, je často také tím, kde jste nejvíce zranitelní.

   66 % odborníků v oblasti bezpečnosti IT si není jistých, kolik zařízení je v jejich prostředí – Evil Things Report | Pwnie Express

4. Začleňte Threat Intelligence – soubor nashromážděných dat a informací, týkajících se bezpečnostních hrozeb, účastníků takovýchto hrozeb, malware a zranitelných míst.

   33 % organizací nemá program Threat Intelligence – Recorded Future

5. Provádějte častá a komplexní hodnocení zranitelnosti proti vašim síťovým zařízením

   99 % uživatelů počítačů je zranitelných k využívání exploit kitu (chyby zabezpečení softwaru). – Heimdal Security

6. Snažte se trénovat a rekvalifikovat své zaměstnance, aby zaznamenali škodlivý provoz. Jednou to nestačí.

   Lidská chyba nebo selhání systému představují 52 % porušení bezpečnosti dat – Security Intelligence

7. Získejte kontrolu nad rozšiřováním VM, bezpečně uchopte BYOD a mobilitu a připravte se na stále rostoucí IoT. Integrita sítě není možná bez komplexního pochopení a kontroly všech prostředků, které se k síti připojují.

   80 % firemních BYOD je "nedostatečně spravováno IT odděleními" - Ovum

O NetSHIELDU

Posláním společnosti NetSHIELD je být důvěryhodným poskytovatelem nákladově efektivních a proaktivních bezpečnostních řešení, které posílí strategie pro snižování rizik v kybernetickém prostředí.