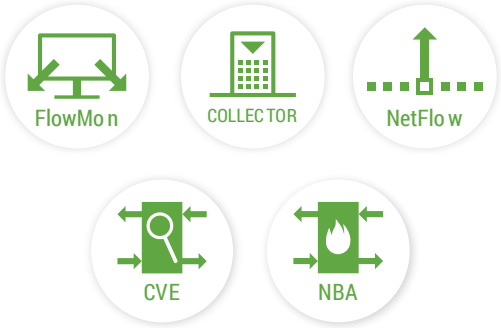
PRODUCT FAMILY



Analýza síťového provozu společnosti

Popis služby

Předmětem nabízené služby je analýza provozu datové sítě společnosti. Spočívá v monitorování datových toků a v následném zpracování získaných dat s cílem poskytnout maximum informací o stavu sítě po stránce provozní a bezpečnostní, a dále s cílem odhalit případné anomálie a bezpečnostní rizika. Součástí analýzy je navržení optimálního rozložení síťových kapacit, určení kritických míst v síti, detekce vnitřních a vnějších útoků a identifikace služeb a uživatelů nejvíce přispívajícím k vytížení datové sítě.

Pro analýzu sítě je využito primárně zařízení společnosti Flowmon, konkrétně sonda s adekvátním výkonem a počtem monitorovacích portů v závislosti na typu a velikosti analyzované sítě. Sonda je zapojena off-line, takže nijak neovlivňuje provoz na síti, a je čistě pasivní, tzn. že do sítě ani mimo ni nic nevysílá. Sonda má minimálně dva porty – do prvního monitorovacího portu (dále označovaného jako LAN) je potřeba zrcadlit provoz všech VLAN procházející přes přepínač, do druhého portu sondy (dále označovaného jako INTERNET) je potřeba zrcadlit provoz linky mezi společností a jejím poskytovatelem přístupu k internetu. Sonda(-y) musí být zapojena(-y) do sítě na dobu minimálně 14 dnů. První týden je věnován sbírání provozních dat pro vytvoření typické úrovně provozu (baseline) a odladění nastavení (zadání rozsahů interních adres, adres serverů, …). Druhý týden se sbíraná data porovnávají s baseline. Na konci monitorovacího období jsou veškerá data vyhodnocena specializovaným software metodou behaviorální analýzy a výsledek zpracován do přehledného PDF reportu. Důležité je říci, že sonda neukládá žádná uživatelská data ani obsah jakýchkoli přenášených zpráv, pouze provozní a lokalizační údaje.

Inventarizace a audit nalezených zařízeních jsou prováděny zařízením Greenbone. Dochází ke skenování sítě v námi zvolených segmentech, díky kterému máme přehled o zařízeních v síti. Na nalezená zařízení dle specifikací zákazníka se aplikuje sada testů, kterými jsou odhaleny bezpečnostní zranitelnosti. Ideální délka nasazení zařízení Greenbone provádějící skenování a testování je minimálně 7 dní pro pokrytí běžného pracovního provozu. Vliv na testované zařízení je závislé na zvolené sadě a detailnosti testů. Podmínkou pro provedení analýzy je poskytnutí nezávislého vzdáleného přístupu na zařízení provádějících analýzu, inventarizaci a testy na zranitelnosti.

V následujících bodech jsou popsány jednotlivé kroky analýzy, které pak odpovídají jednotlivým odstavcům výsledného reportu. V závislosti na požadavcích zákazníka je možné vyhodnocená data odprezentovat, slovně okomentovat, podrobněji vysvětlit a případně i navrhnout kroky pro optimalizaci sítě a zajištění větší bezpečnosti.

Struktura provozu

Obecná charakteristika toku
Porty a služby
Počty komunikačních partnerů

Anomálie a bezpečnostní rizika

Prověření bezpečnostního incidentu
Útoky a infikované stanice
Podezřelé aktivity a rizika
Potenciálně nežádoucí aktivity uživatelů
Provozní anomálie

Inventarizace a audit stanic v síti, včetně auditu zranitelností zjištěných v síti.

DC Product Family - řada produktů společnosti VUMS DataCom, která využívá dlouholetých znalostí trhu a nabízí partnerům a zákazníkům námi speciálně navržená řešení s přidanou hodnotou v podobě znalostní báze a technické podpory.

DISTRIBUTOR PRO ČR:

www.datacom.cz

VUMS DataCom spol. s r.o. | Komplexní řešení datových komunikací | Lužná 716/2 | 160 00 Praha 6 | tel: +420 220 999 511