Konference Communication Security Praha 2020

PRAHA
16. 9. 2020

15. ročník mezinárodní konference o bezpečnosti ICT
Představení nejkritičtějších hrozeb dle ThreatGuard

COMGUARD
communication security

MÍSTO: AQUAPALACE PRAHA, Pražská 138, Čestlice 251 01 Praha - východ **DATUM A ČAS:** Středa 16.9.2020, registrace 8:30, start 9:00

PROGRAM KONFERENCE SÁL THREAT

08:30-09:00
Registrace

09:00-09:10
Úvod

09:10-09:40
ThreatGuard - Máte přehled o aktuálních kybernetických hrozbách?

Víte, že Česká republika je vysoko nad celosvětovým průměrem v počtu evidovaných kybernetických útoků týdně? Expertní služba ThreatGuard poskytuje cenné informace o všech aktuálních kybernetických hrozbách, které na český a slovenský region cílí. Přesvědčte se, jak minimalizovat riziko kompromitace Vaší IT infrastruktury.

Roman Jiráček (COMGUARD)

09:40-10:10
Endpoint Detection and Response (EDR) - pomocník při kybernetickém incidentu

Dnes již víme, že IT bezpečnost není a nikdy nebude stoprocentní. Co ale dělat, dojde-li k incidentu? Klíčové je mít dostatek informací, vybrat to podstatné a správně data interpretovat. S ohledem na množství informací, které může vygenerovat jedna stanice v síti, není možné efektivně řešit bezpečnostní incident. McAfee proto přichází na trh s technologií McAfee Endpoint Detection and Response (EDR), kdy administrátor dostává jen takové informace, které jsou podstatné, a není zahlcován zbytečným šumem.

Martin Votava a Jakub Mazal (COMGUARD)

10:10-10:40
Zabezpečení koncových bodů z pohledu konfigurační zranitelnosti - NOVÁ unikátní technologie

Komplexita správy koncových bodů v posledních letech výrazně narůstá a chybné konfigurace mohou ústit ve vznik kritických zranitelností. Gytpol poskytuje nástroj pro jejich detekci včetně orchestrace nápravných opatření formou jednoduchého agentského řešení s centrálním reportingem a možností integrace se SIEM. Konfigurační zranitelnosti nalezené Gytpol Validatorem bývají přehlíženy antiviry, EDR, Vulnerability Managementy a mnohdy i penetračními testy.

Jan Pawlik (COMGUARD)

10:40-11:00
Přestávka

11:00-11:25
Nemocnice – lákavý cíl pro NEetické hackery

V tomto roce jsme byli svědky mnoha media-lizovaných kyberútoků na zdravotnická zařízení. Mnohá z nich se stala terčem v tu nejméně vhodnou dobu. Seznámíme Vás s hlavními důvody, proč byli útočníci úspěšní a jak se lze efektivně proti těmto útokům bránit např. i s pomocí Sophos XG firewallu.

Petr Konečný a Radek Kugler (COMGUARD)

11:25-11:45
Přesun zranitelností z fyzické infrastruktury do cloudu

Virtualizace fyzické infrastruktury přináší množství benefitů. Migrace serverů do cloudu však neodstraňuje riziko útoků, které je možné ve všech prostředích. Co hrozí nezabezpečenému serveru v cloudu?

Matej Šipkovský (NETVEL)

11:45-12:05
Jak spravovat privilegované účty a přihlašovací údaje?

V době digitální transformace, rozmachu cloudových prostředí a hybridního IT stoupá závratnou rychlostí i množství privilegovaných účtů. Jednou z klíčových oblastí správy rizik a zabezpečení organizace je Privileged Access Management. WALLIX Bastion může být i pro vaší organizaci klíčovým nástrojem pro ukotvení bezpečných přístupových politik a správu životních cyklů přihlašovacích údajů vedoucí ke snížení bezpečnostních rizik spojených se zneužitím účtů s vysokými oprávněními.

Radim Kupka a Lukáš Babčický (COMGUARD)

12:05-12:35
Perimetr sítě se posunul - máte pod kontrolou všechny cloudové služby?

Architektura firemní sítě se v dnešní době výrazně liší od struktur minulých. Stojí za tím zejména rozvoj cloudu. Přizpůsobili jste bezpečnost dat a uživatelů těmto radikálním změnám chápání firemní infrastruktury? Pokud ne, není nejvyšší čas to nyní udělat? S pomocí technologie McAfee Unified Cloude Edge vyřešíte ochranu dat současně v interní infrastruktuře i cloudu. Společně s tím zajistíte i kontrolu nad aktivitami uživatelů na webu a nad cloudovými službami, o kterých jste ani nevěděli, že je zaměstnanci využívají a vystavují tak riziku Vaše citlivá data.

Martin Votava a Michal Mezera (COMGUARD)

Generální parner: McAfee Together is power.

Gold partneři: WALLIX, SOPHOS, RAPID7

Mediální partneři: ChannelWorld, IT Systems www.SystemOnLine.cz

COMGUARD communication security
COMGUARD a.s.
tel. +420 513 035 400
Sochorova 38, Brno
Freyova 27, Praha 9
info@comguard.cz
www.comguard.cz

12:35-13:00

Aktuální bezpečnostní incidenty v kontextu a číslech

Pro potřeby strategického rozhodování je třeba chápat, jak se mění útoky a taktiky útočníků. Je důležité mít představu o možnostech a pravděpodobnosti toho, co mi hrozí. Jenom tak jsou organizace schopné investovat svůj čas a peníze efektivně, správným směrem, a vymanit se z diskuze typu "co když vám tu útočník pohodí flashky s malwarem" a "to určitě chytil někde na pornostránkách". Projdeme společně statistiky útoků a incidentů, a abychom neřešili jenom strohá čísla, ukážeme si i konkrétní příklady. Jedno číslo za všechny - za 70% incidentů mohou externí útočníci, ne interní zaměstnanci.

Robert Šefr

13:00-14:00

Přestávka na oběd

14:00-14:40

Jak zabezpečit spolehlivě Vaši emailovou a webovou komunikaci?

Nejčastějším vektorem vedení kybernetických útoků na firmy a organizace je emailová a webová komunikace. Skrytý malware, jenž je velice obtížné objevit za pomoci běžných bezpečnostních nástrojů, umí napáchat pěknou „paseku". To dokládají i poslední kybernetické útoky zaznamenané na našem území. Proto je zde Lastline Defender, který s pomocí unikátní platformy Network Detection and Response dokáže identifikovat i ten nejpokročilejší malware, jenž by mohl ochromit chod Vaší společnosti.

Roman Jiráček a Jakub Mazal (COMGUARD)

14:40-15:05

SIEM, který pořídíte rychle a levně? Rapid7 InsightIDR

Je opravdu možné pořídit SIEM během několika dní a za částku řádově nižší, než je obvyklé? Odpověď zní ano. Představíme Vám cloudové SIEM řešení výrobce Rapid7 (Gartner Leader) s unikátními možnostmi Log Managementu vyznačující se krátkou dobou implementace, rozsáhlými možnostmi integrací pro efektivní a včasnou investigaci incidentů a reakci na ně.

Jan Pawlik (COMGUARD)

15:05-15:30

Dvoufaktorová autentizace - Jak zajistit bezpečnostní standard a zároveň zvýšit uživatelský komfort?

Autentizace pomocí jednorázových hesel patří dnes již k základním bezpečnostním standardům. Většina aplikací a technologií podporuje přihlášení pomocí OTP, nezřídka dokonce nabízí OTP metody vlastní. To však často znamená ztrátu uživatelského komfortu, kdy se využívají autentizační tokeny per aplikace a tím se logicky pro administrátory navyšují i nároky na správu. Výrobce SecurEnvoy s produktem SecurAccess tyto nedostatky eliminuje. Ukážeme si v praxi, jak snadno se mohou uživatelé autentizovat např. do Windows, VPN nebo cloudových služeb.

Radim Kupka (COMGUARD)

15:30-15:40

Tombola a závěr

PROGRAM KONFERENCE SÁL GUARD

11:00-11:45

Scénář hackerského útoku na firemní infrastrukturu

Vždy Vás zajímalo, jak postupuje útočník při cíleném útoku a chtěli jste to vidět? Nyní máte šanci! Názorně představíme a okomentujeme jednotlivé kroky při plánování, přípravě a samotném útoku v různých jeho fázích, řekneme si o předpokladech a možnostech vedení útoku, i o možnostech obrany.

Jakub Mazal a Michal Mezera (COMGUARD)

12:05-12:35

DNS překlad na doménové řadiče nepatří

Nechávat překlad nebo přesměrování dotazů na externí domény na doménových řadičích se ukazuje jako velké riziko, přesto je to téměř standard ve většině menších a středních organizacích. Kromě toho, že doménové řadiče řeší překlad domén jen do té míry, aby nějak fungoval, tak služba na serveru běží s oprávněním SYSTEM. Pokud útočník službu úspěšně exploituje, stane se vládcem celé vaší sítě. Zranitelnost SIGRed tento problém v architektuře sítě odhaluje v celé nahotě a je dalším dílem do skládačky možnosti zneužití DNS provozu a protokolu. V příspěvku se podíváme, jakým způsobem je možné DNS překlad efektivně řídit a auditovat.

Robert Šefr (Whalebone)

11:45-12:05

Nové možnosti investigace v rámci Sophos EDR

Jak snadno analyzovat zachycený incident a zjistit souvislosti? Řešením je Sophos Endpoint Detection and Response (EDR) ve verzi 3.0, které přináší řadu novinek. Ze Sophos Central management konzole můžete na koncových strojích např. nalézt podezřelé procesy a odhalit, na jaké IP adresy a přes jaké porty komunikovaly, a následně aplikovat nápravná opatření. Vše podpoříme živou ukázkou.

Petr Konečný a Radek Kugler (COMGUARD)

12:35-13:00

SIEM řešení pro fajnšmekry - LogRhythm

Proč dávat události v síti do souvislosti s uživateli? Kolik času ušetří umělá inteligence při běžné práci se SIEM a následné investigaci? Představíme si možnosti pokročilého UEBA s využitím komponenty Cloud AI. LogRhythm nekončí pouze u odhalení incidentu, ale nabízí i kompletní modul SOAR, jenž umožňuje zavést automatické reakce na základě předdefinovaného workflow. Předvedeme Vám, jak to celé funguje v praxi.

Martin Votava a Jan Pawlik (COMGUARD)

ZMĚNA PROGRAMU VYHRAZENA.

TĚŠÍME SE NA VAŠI ÚČAST,

Tomáš Mačica & tým COMGUARD a.s.
marketing@comguard.cz