HackFest 2020

9. september 2020 | HubHub - Twin city C | Bratislava

8:30 - 9:00	**Raňajky a voňavá káva**
9:00 - 9:15	**Privítanie a otvorenie konferencie HackFest 2020.** *Tomáš Valenta, ASBIS*
9:15 - 10:00	**Would you like some RCE with your Guacamole?** *Eyal Itkin, Check Point* The outbreak of the COVID-19 pandemic, had deeply impacted us all, and led to a transition from onsite to off premise work. This change means that IT solutions for remote work are now widely used, making them a prime target for attackers. In our research, we focused on Apache Guacamole, a popular such infrastructure, and discovered that it contains critical Reverse RDP Vulnerabilities. These vulnerabilities allow an attacker, who has a foothold inside the network, to launch an attack on the gateway when an unsuspecting worker tries to connect to an infected machine. Once exploited, the actor can intercept and control all of the sessions, effectively controlling the entire organization.
10:00 - 10:30	**História hackingu.** *Andrej Aleksiev, Check Point* Od prvého pomenovania týchto aktivít prešlo 60 rokov. Inými slovami, v dnešnej dobe pozorujeme už 3. generáciu hackerov, ktorí sú úplne odlišní od tých pôvodných. Dnešná generácia sa odlišuje nielen technikami, ale aj myslením. Pozrime sa na vývoj a taktiku jednotlivých generácii...
10:30 - 11:00	**Nástroj pre automatizované testovanie zraniteľnosti a úrovne zabezpečenia IT infraštruktúry.** *Karel Ružička, NTT* Pri súčasnom raste komplexnosti a rozsahu IT sietí v kombinácii s akútnym nedostatkom kvalifikovaných ľudských zdrojov je nasadenie automatizácie jedným z možných riešení, ktoré pomôže správcom efektívne znižovať úroveň zraniteľnosti ich IT systémov a zvýšiť ich zabezpečenie proti kybernetickým útokom. Aké sú funkčné rozdiely a vlastnosti automatizovaného testovacieho nástroja v porovnaní s tradičnými riešeniami a nástrojmi určenými pre penetračné testovanie a vulnerability scanning?
11:00 - 11:30	**Prestávka**
11:30 - 12:00	**Pokročilá aktívna ochrana proti malware a ransomware. Ako ochrániť zariadenie pomocou aktívnej aj pasívnej ochrany?** *Jan Ptáček, Aleš Hok, ACRONIS* Môžete sa tešiť na živú ukážku phishingového ransomwarového útoku a jeho zastavenie. Predvedieme vám unikátnu funkcionalitu – skenovanie a odhalenie malware v zálohách a zároveň sa pozrieme na to, aké sú možnosti zálohovania, obnovy, disaster recovery a patch managementu s riešeniami Acronis.
12:00 - 12:30	**Jednoduchá a efektívna ochrana nielen Check Point VPN s využitím modernej MFA.** *Pavol Sýkora, Peter Matuška, ANECT* Myslíte si, že je phishing zložité uskutočniť? Myslíte si, že Vás sa phishing netýka? 80% útokov využíva slabé či ukradnuté heslá. V živej prezentácii Vám ukážeme, ako najrýchlejšie a užívateľsky najprívetivejšie ochrániť Vaše prihlásenie do Check Point VPN.
12:30 - 13:00	**Bezpečnosť RFID kariet.** *Juraj Nemeček, Juraj Belko, TEMPEST* Hľadáte odpoveď na otázky, čo je RFID a kde všade sa používa? Aký HW/SW sa používa pri auditovaní a analýze? Do akej miery je zraniteľná prístupová karta, ktorú mám vo vrecku? Nemusíte sa báť, spoločne sa pozrieme na prípady nasadenia jednotlivých technológií a praktické hacky s ukážkou používaného HW/SW. Získate základný prehľad, ktorý typ kariet môže byť emulovaný alebo dokonca klonovaný.
13:00 - 14:30	**Obed**
14:30 - 15:00	**Zraniteľnosť, ktorá odkryla komunikáciu vyše miliardy Wi-Fi zariadení.** *Filip Mazán, ESET* ESET objavil doposiaľ neznámu zraniteľnosť vo Wi-Fi čipoch, ktorá zapríčiňuje nesprávne šifrovanie časti sieťovej komunikácie takzvaným nulovým kľúčom. Chyba nesie názov Kr00k a týka sa zariadení, ktoré používajú populárne Wi-Fi čipy od spoločností Broadcom, Cypress, no potenciálne aj od ďalších výrobcov. Celkovo ide o viac ako miliardu zariadení, vrátane výrobkov spoločností Apple, Samsung, Google či Amazon. Kr00k okrem nesprávneho šifrovania tiež spôsobuje, že zraniteľné zariadenie zle zabezpečené dáta vyšle „do vzduchu", kde je možné ich odchytiť. Zraniteľnosť by mohli útočníci zneužiť na sledovanie Wi-Fi komunikácie obeti a krádež jej dát a to aj v prípade, že sieť používa protokol WPA2.
15:00 - 15:30	**Umenie tvorby exploitu - bluekeep.** *Tomáš Vobruba, Check Point* Nedávno som sa stretol so situáciou, kde som musel zákazníkovi pripraviť exploit bluekeepu a dokladovať mu, že naše riešenie ho dokáže zastaviť. Pozrime sa, ako som na základe všeobecne dostupných informácií na internete, dokázal z nefunkčného dema bluekeep zraniteľnosti, vytvoriť plnohodnotný exploit s payloadom na remote shell.
15:30 - 16:00	**Check Point CloudGuard SaaS - ochrana SaaS a cloud aplikácií.** *Andrej Mišík, ASBIS* CloudGuard SaaS je cloudová služba pre zabezpečenie SaaS služieb, ako sú Office 365, One Drive, Gsuite Email, alebo Google Drive. V živej ukážke predvedieme ochranu týchto SaaS aplikácií nad rámec Cloud Access Security Brokera nielen pred neznámymi hrozbami, ale aj pred únikom korporátnych dát, identít užívateľov, phishingu a ďalšími typmi moderných útokov.
16:00 - 16:15	**Ukončenie prezentácií, vyhodnotenie Cyber Challenge**
Od 16:15	**Občerstvenie a networking**

ESET Acronis Check Point SOFTWARE TECHNOLOGIES LTD. ASBIS SUCCESS THROUGH FOCUS

Kontaktná osoba: Adriena Némethová | +421 907 964 682 | nemethova@asbis.sk