FUTURE FORCES FORUM
International Platform for Trends & Technologies in Defence & Security
www.future-forces-forum.org

FUTURE OF CYBER CONFERENCE 2016

CYBER TRENDS

3rd edition of Future Cyber Security & Defence Conference

20 – 21 OCTOBER 2016

General Partner: Deloitte.

Conference Partners: Microsoft, CYBERGYM EUROPE EXPECT THE UNEXPECTED, net pointers communications, Fidelis Cybersecurity, FORTINET

Cyber Pavilion Sponsor: GORDIC

Topic Sponsors: secunet, CISCO

Partner Slot & TT: AEC, Intel Security, Allied Telesis

Cyber Workshops Partners: NSM, AXENTA, ESET, navicom, Microsoft, CZ.NIC, Deloitte., GORDIC

CYBER TRENDS is a two-day International professional conference divided into four sections accompanied by live demonstration and simulation test area, professional workshops and Table-top exhibition of partners' solutions and products. The conference is a part of international project FUTURE FORCES FORUM which includes set of EXPERT EVENTS and the International defence and security exhibition FUTURE FORCES 2016.

The conference will be held in Prague, capital of the Czech Republic. The conference is primarily aimed at the security and information community of the public sector, armed and security forces, the academia and private business cooperating in projects of public interest. The conference is focused on developing international cooperation in cyber security in Europe, with special focus on the Czech Republic, Slovak Republic, Hungary and Poland.

It is expected that more than 500 professionals will participate, including representatives from NATO, European Union and other international institutions.

Executive Guarantor: AFCEA

In cooperation with

CONFERENCE PATRONAGE & SUPPORT, HONORARY CHAIRMEN

Mr. Dušan NAVRÁTIL, Director, National Security Authority, Czech Republic

Mr. Milan CHOVANEC, Minister of Interior, Czech Republic

Mr. Martin STROPNICKÝ, Minister of Defence, Czech Republic

MGen. Erich STAUDACHER Deputy Director of the Bundeswehr Planning Office, Germany

BGen. Prof. Bohuslav PŘIKRYL Rector, University of Defence, Czech Republic

Assoc. Prof. Jozef PUTTERA Rector, Armed Forces Academy of General Milan Rastislav Štefánik, Slovakia

Assoc. Prof. Josef SALAČ Rector, Police Academy Prague, Czech Republic

Assoc. Prof. Lucia KURILOVSKÁ Rector, Academy of the Police Force in Bratislava, Slovakia

Mr. Petr JIRÁSEK Chairman, AFCEA Czech Cyber Security Working Group, Czech Republic

CONFERENCE PROGRAMME COMMITTEE MEMBERS

Mr. Jaroslav BURČÍK Director, ITU Centre of Excelence for Cyber Security, Czech Technical University, Czech Republic
BGen. Ľubomír GACKO Chief of the Operations Support Staff; General Staff of the Armed Forces of the Slovak Republic, Slovakia
Col. Ľubomír GORELČÍK Chief CIS Branch, J6 of General Staff of the Slovak Republic, Slovakia
Assoc. Prof. Marcel HARAKAĽ Vice-rector, Armed Forces Academy, Slovakia
LtCol. Petr HRŮZA University of Defence, Czech Republic
BGen. Jan KAŠE Chief of Military Office, Military Office of the President of the Republic and Castle Guard, Czech Republic
Col. (Ret.) Ladislav KOLLÁRIK Vice-president, AFCEA Slovak chapter, Slovakia
Mr. Tomáš MÜLLER President, AFCEA Czech Chapter, Czech Republic
Mr. Vladimír ONDROVIČ President of the Union of Electrotechnical Industry and AFCEA Slovak Chapter, Slovakia
Mr. Jaroslav PEJČOCH Member, Management Committe for Information Society ICT UNIE, Czech Republic
Assoc. Prof. Josef POŽÁR Dean, FSM, Police Academy Prague, Czech Republic
Mr. Vladimír ROHEL Director, National Cyber Security Centre, Czech Republic
LtCol. (Ret.) Josef STRELEC Honorary President, AFCEA Czech chapter, Czech Republic
BGen. Miloš SVOBODA Deputy Director, Fire Rescue Service, Czech Republic
MGen. (Ret.) Klaus-Peter TRECHE General Manager, AFCEA Europe, Germany
Mr. Josef VESELÝ Security Director, Ministry of Interior, Czech Republic

General Partner of Future Forces Forum: LOM PRAHA
General R&D Partner of Future Forces Forum: CZECH TECHNICAL UNIVERSITY IN PRAGUE
Partner of Future Forces Forum: VOP CZ
General Partner of FCC: Deloitte.
LCWS Platinum Partner: HUTIRA CCW
Main Technical Partners: sorsya, YVENTECH
Services Partners: VIENNA HOUSE DIPLOMAT PRAGUE, volarena
CEBIRAM Platinum Partner: PHILIPS
CBRN Workshop Platinum Partner: FUTURETECH, Kärcher Group
MARS Platinum Partner: VTÚ

Under the Auspices of

Endorsed by

Bezpečnost v praxi a pro každého

V současnosti se stále mluví o bezpečnosti, ochraně dat, šifrování a dalších, pro normálního člověka nepodstatných věcí. Proč by nás to mělo trápit? Máme přece na starosti důležitější věci. Opravdu?

Začněme příměrem. Pokud vám do bytu vtrhne parta zlodějů a byt vykradou, je to k naštvání. Zpravidla vylomené dveře, nepořádek, ztráta osobního majetku (část, ke které je nějaké citové pouto nenahraditelná penězi), nutnost nahradit chybějící doklady, která znamená spoustu běhání po úřadech. Řešením jsou bezpečnostní dveře, elektronické zabezpečení. Internet a současné formy komunikace tak trochu připomínají v ochraně dat divoký západ. Pro většinu lidí je nemožné dodržovat pravidla, o jejichž existenci nemají ani tušení. Navíc ani nemají důvody proč se chránit. A snaha o osvětlení těchto důvodů vedla k tvorbě tohoto článku.

Žijeme v informační společnosti. Každá naše aktivita zanechává stopu v systému. Nemyslím tím jakýsi všeobjímající Matrix, ale velké množství vzájemně spolupracujících databází. Jednou stopou je platba v obchodě. Druhou je telefonát manželce či dítěti. Zápis na katastru, evidence ve škole, platba faktur mezi obchodními partnery, průjezd křižovatkou či úsměv do kamery v metru. Všechny tyto informační systémy sbírají data. A ta je možné vytěžit a zneužít.

Chcete se dozvědět více. Pokračujte ve čtení na *www.ict-nn.cz*

Více si přečtete na:

Gartner Magic Quadrant 2016 pro oblast SIEM nástrojů

...pokračování na straně 1

Nyní to přední výrobci SIEM nabízí jako interní funkcionalitu.

- **Kontextově obohacené události** – umět zpracované log data v události zkombinovat s kontextovými informacemi jako jsou uživatelé, ICT komponenty a jejich zranitelnosti, potenciální nebo již proběhlé hrozby. Obvykle to bylo v dřívějších SIEM systémech zajištěno až systémovým integrátorem úpravami dat v pre-procesing fázi a implementací dodatečných korelačních scénářů či specifických reportů.
- **Analýza chování uživatelů a komponent (UEBA, User and Entity Behavior Analytics)** – detekce a lokalizace anomálních odchylek od průměrného nebo standardního trendu je v bezpečnosti používána delší dobu. Nyní bývá interní součástí detekčních funkcí SIEM, což výrazně zlepšuje detekční schopnost pro sledování chování uživatelů a sledování provozně bezpečnostních parametrů ICT komponent. Uživatelé se obecně umějí chovat značně nevyzpytatelně, a detekce „přirozené stupidity" uživatelů nebyla silnou stránkou žádného software, ani toho vybaveného silnou „umělou inteligencí". S nárůstem počtu připojovaných koncových komponent (vzrůstá trend připojených notebooků, smart-device) se detekční algoritmy, sledující anomální chování, synergicky používají i k lokalizaci problémových komponent. A logicky lokalizaci jejich vlastníků (taky problémových).
- **Efektivnější normalizace dat** – umět korelovat a analyzovat data z různě dostupných zdrojů pro sledování datové sítě, chování uživatelů, chování komponent sledovaného prostředí, pro naplnění souladu s legislativou či specifické účely vyšetřování na základě analýz historických trendů, dotazů na specifické informační vazby.

Magic Quadrant (téměř) beze změn

Oproti roku 2015 nám rok 2016 nepřinesl dramatické změny, kdy na top pozicích je klasická sestava top SIEM nástrojů:

1. IBM QRadar (1. Pořadí ve 2015)
2. Splunk (2. Pořadí ve 2015)
3. LogRhythm (5. Pořadí ve 2015)
4. HPE ArcSight (3. Pořadí ve 2015)
5. Intel Security (4. Pořadí ve 2015)

O tom, podle čeho vybírat SIEM nástroje se dočtete na *www.ict-nn.cz*.

Více si přečtete na:

Přední datový vědec NIST: Potřebujeme nový přístup k IT

Ron Ross: Je třeba nový přístup k návrhu a prodeji počítačových systémů. Musí být navrženy od základů jako bezpečné.

Bezpečnostní software, firewall, detekce anomálií nebo jiné systémy nemohou chránit IT infrastrukturu, jež je z principu nedůvěryhodná. Potřebujeme nový přístup k počítačové architektuře a bezpečnosti. Jen tak se vypořádáme s kybernetickou krizí, pronesl Ron Ross, bezpečnostní analytik prezidentské komise a poradního výboru pro NIST na konferenci Enhancing National Cybersecurity, zřízené pro řešení problémů s kyberbezpečností.

„Pro řešení hrozící kybernetické krize je třeba vytvořit více důvěryhodné bezpečné komponenty a systémy," řekl Ross. *„Kyberbezpečnosti věnujeme více zdrojů než kdykoliv v historii, a přesto jsme svědky rostoucího počtu úspěšných kybernetických útoků. Bezpečnost, jakou v současnosti máme, na místě nefunguje. Nemůžeme tedy chránit to, co to nechápeme. Zvýšená složitost se promítá do zvětšení možných příležitostí k útoku. Výsledkem je ztráta omezení a rostoucí příležitosti pro hackery, jak využít zranitelností plynoucích z nedostatků v softwaru, firmwaru a hardwarových komponentách základních systémů a sítí. Jak se organizace a uživatelé snaží najít a opravit známé zranitelnosti, počet neznámých roste, stejně i komplikovanost systémů, která bude složitější, pokud bezpečnost bude stále takto nastavena. Současný přístup neřeší základní nedostatky v systémové architektuře a designu."*

Ross volá po novém přístupu stavby více důvěryhodných a bezpečných komponent a systémů, uplatňováním definovaných konstrukčních principů bezpečnosti v rámci konstrukčního i životního cyklu zařízení. *„Zabezpečení se nestane samo od sebe,"* řekl. Bezpečnost a spolehlivost musejí být navrženy od začátku, s přirovnáním k procesu disciplinovaného a strukturovaného přístupu, používaných pro návrh letadel.

Vysoce zabezpečená a důvěryhodná řešení nemusejí být vhodná vždy, ale měly by být k dispozici pro kritické subjekty, důležité pro zájmy USA: řízení rozvodné soustavy, výrobní závody, finanční instituce, doprava, čistírny odpadních vod a zbraňové systémy. *„Nový přístup vyžaduje značné investice zdrojů a nových partnerství, včetně vlády, průmyslu a akademické obce,"* řekl Ross, přirovnávaje ho k projektu Apollo z roku 1960.

Jan Dušátko

Více si přečtete na: