

Agenda konference

Partneři - ČAP, Principal engineering, ICTUnie, Microsoft, Munich Re, Zentrum für Risiko- und Krisenmanagement, MARSH, Deloitte Advisory, QNI, ČVUT, Boxtrap Security a Data Security Services

Mediální partneři - OPojíštění.cz, MM - Průmyslové spektrum, ITSsystems

Cyber Insurance Conference 2019

Digitální transformace ekonomiky přináší nová kybernetická rizika. Jak mohou pojišťovny pomoci a jak je na to připravit?

Moderuje : Lucie Nová

13. 6. 2019 konferenční centrum Microsoft Praha, Vyskočilova 1561/4a

		Agenda	Vystupují
8:30	9:00	Registration - Warming Up	
9:00	9:10		
	0:10	Úvod - Welcome speach	Jan Matoušek, Výkonný ředitel České asociace pojišťoven
9:10	9:30	Zaměřujeme se na digitalizaci státu, ekonomiky a služby občanům. Jak vnímáme kybernetickou bezpečnost a roli pojišťoven. Jak může společně fungovat nová legislativa, prevence, technická opatření a také pojištění.	Mgr. Zdeněk Zajíček, Prezident ICT Unie
	0:20	Stát má silnou koncepci digitalizace svých aktivit a služeb občanům. Stejně tak podporuje technologický rozvoj firem a zvyšování jejich konkurenceschopnosti. Jaké je místo pro řízení kybernetických rizik? A kde může být prostor pro spolupráci s pojišťovnami?	
9:30	9:55	From risks to opportunities. Který rok bude rokem Cyber insurance – 2019 just hype? Which year is going to be the year of cyber insurance?	Martin Kreuzer, Munich RE, Corporate Underwriter Cyber Risks, Munich, Germany
	0:25	Nikdo nepochybuje o businessový potenciál, který má pro všechny aktéry pojištění kybernetických rizik. Proč se ale prodává jako šafrán, zejména v porovnání s klasickými produkty? Proč, když rizika i reálné dopady tu jsou? Podívejme se na kontext problému a vybraná úskalí i možná řešení No one challenges the business potential that cyber risk insurance has for all involved parties. But why is it not exactly selling like hot cakes, especially when compared to traditional products? Why, when there are risks and real impacts? Let's look at the context of the problem and the pitfalls and possible solutions.	
9:55	10:25	Pojištění kybernetických rizik: Jaký je vztah mezi riziky dodavatelského řetězce a kybernetickými riziky. Jaký je stav v národní a mezinárodní normalizaci. Cyber Insurance: Correlation between Supply Chain Network Risks and Cyber Risks- Representation of the status quo in the national and international Standardization	Jochen Ressel, Dipl.-Ing. Dr.techn. Thomas Schaberreiter, Dr. Wolfgang Reisinger, Zentrum für Risiko- und Krisenmanagement, Vienna, Austria
	0:30	Dnešní výrobci a dodavatelé služeb musí spoléhat na své dodavatele. Dodavatelské řetězce jsou však zdrojem častého rizika. Jak by měly odběratelé reagovat na tyto kybernetické hrozby? Jak to dnes řeší standardy pro ošetření rizik?	
10:25	10:30	MINI Panel - Čas na dotazy	
	0:05	Čas na pár otázek k přednášejícím	
10:30	11:00	Coffee Break	
	0:30		Příležitost k networkingu
11:00	11:20	Bezpečnost jednotlivých uživatelů je podmínkou pro bezpečný svět. Může twnto náročný úkol globální Microsoft vůbec zvládnout?	David Šostý, Microsoft
	0:20	Zaměřujeme se na to, jak zajistit progresivní řešení, nasazení nových technologií, komfortní a přitom bezpečné služby uživatelům ve různých segmentech.	
11:20	11:40	Co uvidíte, když se podíváte firmě pod kybernetické sukne? Aneb cudnost kybernetickým rizikům nesluší.	Jan Seidl, Delloite
	0:20	Aby nebyla analýza firemních kybernetických rizik jen formalita, musí být poměrně důkladná a jít pěkně pod kůži. Jedině tak je možné odhalit slabá místa. Víte na co si musíte dát pozor?	
11:40	12:00	Je audit informační či kybernetické bezpečnosti jen ztráta času?	Richard Veselý, expert na audit a kybernetickou bezpečnost
	0:20	Kybernetická rizika je potřeba správně identifikovat a řídit v rámci finančních možností společnosti. At' už provádíte audit pravidelně nebo namátkově je potřeba vybrat kvalitního auditora a vytěžit průběh i výstupy auditu na maximum. Audit má primárně ukázat zda Vaše kontroly mapované na rizika fungují a mají smysl, ale můžeme z auditu získat i více? Jak má takový audit vypadat a jak ne? Co se někdy podaří najít při auditu?	
12:00	12:25	Na veřejnost se sice dostanou jen ty největší kybernetické incidenty. Na pojišťovnu se ale pojištěné firmy obracují poměrně často. Jak by pojišťovna měla tyto kybernetické pojistné události likvidovat?Only the biggest cyber-incidents have wide public awareness. However, insured companies turn to the insurance company quite often. How should an insurance company manage claims resulting from these cyber events?	Thomas Marcadet, MARSH, Vienna, AUSTRIA
	0:25	Případové studie na základě reálných případů úpisů likvidace kyber pojistné události z různých oblastí Praktické rady a tipy, co potřebují pojišťovny a makléři k úspěšnému úpisu pojištění, a co k úspěšné likvidaci pojistných událostí?	
12:20	12:25	MINI Panel - Čas na dotazy	
	0:05	Čas na pár otázek k přednášejícím	
12:25	13:15	Oběd	
	0:50		Příležitost k networkingu
13:15	13:35	Digitalizace průmyslových firem vstoupila do nové etapy Průmyslu 4.0. Vedle pokroku však přináší i nová rizika o kterých se zatím moc nemluví.	Tomáš Hejlík, QNI
	0:20	Průmysl je páteří ekonomiky. Rizika jsou poměrně vysoká, kybernetická bezpečnost je komplexní obor a kondice zařízení a systémů potřebám doby už mnohdy neodpovídá. Kde jsou dnes v průmyslových podnicích skryta závažná rizika a na co si dát pozor?	
13:35	13:55	Soudní zناletví je skoro jak detektivka. Jak se v kybersvětě posuzují věci, které jsou zdánlivě neviditelné?	doc. Ing. Zdeněk Lokaj, Ph.D, ČVUT FD, Ústav aplikované informatiky v dopravě
	0:20	Soudní zناletví pomáhá řešit spory při likvidaci pojistné události. Jak posuzování kybernetické události probíhá, co ještě lze a co již nelze posuzovat. A co vás také může při posuzování překvapit.	
13:55	14:15	Nová řešení pro kybernetickou bezpečnost - jak se zajetí vysokých nákladů a přílišné složitosti cyber-security.	Dušan Mondek, Rozálie Ryčlová, BoxTrap
	0:20	Desítky bezpečnostních produktů, tisíce bezpečnostních alertů každý den a nikdo, kdo by se postaral o jejich prověření. Běžný obrázek většiny dnešních korporací, kde složitost, náklady na IT bezpečnost a nedostatek kvalifikovaného personálu představují nový typ rizik, kterým je třeba čelit. Přednáška se bude týkat tématiky užiti AI v pro kybernetickou bezpečnost, Security Orchestration, Automation & Response (SOAR) a ochrany firemních procesů.	
14:15	14:35	Když potřebujete vědět, kolik může kybernetické riziko stát vlastně peněz. Jak nejpřesněji určit výši možných škod?	Tomáš Pavlis, Tomáš Havelka, Data Security Services
	0:20	Dnes vůbec není jednoduché vyčíslit, o kolik může firma při kybernetickém incidentu přijít. Kdo to dokáže, bude mít výhodu při popisu rizik a úpisu pojistek. Pojďme se podívat na úspěšnou metodu FAIR a předvedení na praktických příkladech.	
14:35	15:05	Panel - Čas na dotazy	Přítomní přednášející
	0:30	Čas na pár otázek k přednášejícím	
15:05	0:00	Také away... Co si z konference odnést? Finální myšlenky a shrnutí konference	

Změna programu vyhrazena