EUROPEAN CLUSTER COLLABORATION PLATFORM

Collaborate to protect: Network intelligence for cybersecurity

Summary

EUCLUSTERS TALKS

EU Clusters Talks
18 October 2023, 8:30 – 9:45 CET

An initiative of the European Union

Spolupracujte na ochraně: Síťové zpravodajství pro kybernetickou bezpečnost

SHRNUTÍ

European Cluster Collaboration Platform zorganizovala přednášku EU Clusters Talk, která proběhla 18. října 2023 a jejímž cílem bylo zvýšit povědomí o důležitosti ochranných mechanismů a zjistit, jak malé a střední podniky a klastry řeší kybernetickou bezpečnost ve svých sítích.

Program přednášky:

Moderátorka: Chris Burns

1. ECCP novinky
   ***Nina Hoppmann**, členka týmu, ECCP*
2. Politiky EU v oblasti kybernetické bezpečnosti
   ***Boryana Hristova-Ilieva**, Právní poradce, DG CNECT, Evropská komise*
3. Panelová diskuze
   ***Filippo Bosi**, CEO, Imola Informatica, viceprezident, Clust-ER Innovate*
   ***Miroslav Lučinskij,** CEO, kritická ochrana, člen BCCS Cluster*
   ***Stelian Brad**, profersor Inteligentní robotika a inovační inženýrství, prezident, Cluj IT Cluster*
   ***Teofilo Redondo**, manažer technologií a inovací, Bidaidea, člen AEI Ciberseguridad*
4. Možnosti financování
   ***Nina Hoppmann**, členka týmu ECCP*

Klíčová sdělení

- Zákon o kybernetické odolnosti se bude týkat 99 % výrobců hardwaru a vývojářů softwaru na trhu EU.
- Provozní odolnost a robustní rámce jsou klíčem k bezpečnosti malých a středních podniků před kybernetickými útoky.
- Základní nástroje, informovanost a vzdělávání jsou potřebné na všech úrovních organizace.
- Červené týmy a specifické nástroje mohou pomoci v přípravě, protože simulují útoky a pomáhají procvičovat obranné strategie v kontrolovaném prostředí.
- Technology advancements mean a constant adaptation of an organisation's cybersecurity policies.

1. Politiky EU v oblasti kybernetické bezpečnosti

Nina Hoppmann, členka týmu ECCP

Po úvodním slovu moderátora Chrise Burnse byly představeny následující novinky:

1. Veřejná konzultace: Požadavky na podávání zpráv pro podniky a členské státy s cílem snížit administrativní zátěž
2. Online školení na téma "InvestEU v akci" nabízené sítí Enterprise Europe Network.

3. Pozvánka k účasti na Evropském týdnu malých a středních podniků 2023 ve španělském Bilbau.
4. Pozvánka k účasti na Týdnu evropských surovin 2023 v Bruselu.
5. Registrace k účasti na příštích akcích "Clusters meet Regions".
6. Připojte se k diskusním skupinám ECCP na síti LinkedIn.

2. Nová evropská iniciativa Bauhaus

Boryana Hristova-Ilieva, Právní poradce, DG CNECT, Evropská komise

Boryana Hristova-Ilieva vysvětlila vývoj právních předpisů EU v oblasti kybernetické bezpečnosti, počínaje směrnicí NIS (Network and Information Systems) z roku 2016, která stanovila základní protokoly kybernetické bezpečnosti v celé EU. Tato směrnice vyžadovala, aby členské státy vytvořily vnitrostátní orgány a strategie kybernetické bezpečnosti. Směrnice NIS 2, která vstoupila v platnost v lednu 2023, aktualizuje původní směrnici NIS a řeší zvýšená rizika v oblasti kybernetické bezpečnosti a digitalizace, která byla urychlena událostmi, jako je COVID-19 a válka na Ukrajině. Obsahuje ustanovení o řešení incidentů, kontinuitě provozu a bezpečnosti dodavatelského řetězce. Třemi hlavními pilíři jsou schopnosti členských států, řízení rizik a podávání zpráv a spolupráce a výměna informací. Směrnice NIS 2 věnuje zvláštní pozornost malým a středním podnikům, začleňuje je do vnitrostátních strategií kybernetické bezpečnosti a zajišťuje jim podporu a pomoc. Uznává zásadní úlohu malých a středních podniků v ekonomice a jedinečné výzvy, kterým v oblasti kybernetické bezpečnosti čelí.

Zákon o kybernetické odolnosti byl navržen v září 2022. Cílem tohoto zákona je posílit bezpečnost dodavatelského řetězce stanovením standardů kybernetické bezpečnosti pro výrobky s digitálními prvky, a to od fáze návrhu až po vývoj. Zákon navrhuje pravidla kybernetické bezpečnosti pro uvádění hardwaru a softwaru na trh (objektivní, technologicky neutrální a na riziku založené základní požadavky na kybernetickou bezpečnost) a definuje povinnosti výrobců, distributorů a dovozců. **Zákon bude relevantní pro 99 % výrobců hardwaru a vývojářů softwaru na trhu EU a bude mít pozitivní dopad na konkurenceschopnost a vnitřní trh.** Odhad snížení počtu kybernetických bezpečnostních incidentů pro podniky se pohybuje mezi 20 % a 33 %.

Boryana Hristova-Ilieva zdůraznila, že EU nabízí různé mechanismy podpory pro malé a střední podniky, včetně programů Horizont Evropa, Digitální Evropa a digitálních inovačních center. Cílem je posílit kybernetickou bezpečnost a zároveň chránit a podporovat průmysl.

3. Panelová diskuze

Panelisté diskutovali o výzvách a strategiích v oblasti kybernetické bezpečnosti pro malé a střední podniky, o existujících nástrojích a spojování sil pro řešení kybernetických útoků, o potřebě vzdělávání na všech úrovních organizace a o vládních programech a nařízeních pro silný rámec.

Hlavním tématem diskuse byla provozní odolnost, která je pro malé a střední podniky obzvláště důležitá. Filippo Bosi zdůraznil, že je třeba, aby malé a střední podniky vytvořily robustní rámce, které jim umožní nejen odolat kybernetickým útokům, ale také zachovat obchodní činnost během takových událostí. Z jeho zkušeností, které čerpal z dlouholetého poradenství v oblasti finančních služeb, vyplývá, že jen málo malých a středních podniků

je skutečně připraveno a že je pro ně nezbytné mít zavedený systém, zejména s postupující digitalizací.

Miroslav Lučinskij představil nástroj "Cyber Range", virtualizované prostředí vyvinuté na základě spolupráce univerzit a firem. Tento nástroj je navržen tak, aby malým a středním podnikům umožnil simulovat a procvičovat obranné strategie v kontrolovaném prostředí, které odráží praktické potřeby těchto podniků při řešení kybernetických bezpečnostních hrozeb. Obecně může být koncept red teamingu účinnou strategií pro testování a posilování kybernetické obrany organizace. Tento přístup, který zahrnuje simulované kybernetické útoky, pomáhá organizacím identifikovat zranitelná místa a zlepšit jejich bezpečnostní opatření.

Všichni řečníci jsou členy klastrů a shodli se na tom, že klastry jako sítě spolupráce mohou pomoci vytvořit podpůrné prostředí pro malé a střední podniky v oblasti kybernetické bezpečnosti. Klastry umožňují sdílení znalostí, zvyšování povědomí a přístup k základním nástrojům a zdrojům. Překlenují propast mezi akademickou sférou a průmyslem a vytvářejí synergickou platformu pro řešení problémů kybernetické bezpečnosti.

Řečníci také zdůraznili nutnost základních nástrojů, jako jsou správci hesel, a důležitost informovanosti zaměstnanců pro prevenci útoků. Tyto základní prvky jsou často přehlíženy, ale mají zásadní význam pro vybudování silné první linie obrany proti kybernetickým hrozbám. Všichni řečníci zdůraznili význam informovanosti a školení v oblasti kybernetické bezpečnosti na všech organizačních úrovních. Vzdělávání zaměstnanců a odborníků v oblasti potenciálních kybernetických hrozeb a vhodných reakcí je zásadní pro udržení bezpečného digitálního prostředí.

Účastníci panelu dále zdůraznili význam zavedení důkladných politik kybernetické bezpečnosti v organizacích. Tyto politiky poskytují strukturovaný přístup k řízení a zmírňování kybernetických rizik a jsou v souladu s osvědčenými postupy a regulačními požadavky. Při pohledu na rychlý rozvoj umělé inteligence a její potenciální dopady na kybernetickou bezpečnost zdůraznili panelisté potřebu neustálé ostražitosti a přizpůsobování strategií kybernetické bezpečnosti, aby držely krok s technologickým pokrokem.

Za klíčové pro zvýšení kybernetické bezpečnosti malých a středních podniků byly označeny vládní podpora a účinné předpisy. Účastníci panelu uváděli příklady, jako jsou izraelské vládní programy vzdělávání v oblasti kybernetické bezpečnosti a význam kybernetického pojištění, které ukazují, jak iniciativy shora dolů mohou významně ovlivnit kybernetickou bezpečnost malých a středních podniků.

V souvislosti s finančními omezeními, kterým malé a střední podniky čelí, navrhli řečníci řešení, jako je sdílení nákladů prostřednictvím klastrů a přístup k bezplatným nástrojům nebo nástrojům s otevřeným zdrojovým kódem. Tyto přístupy mohou malým a středním podnikům pomoci zahájit opatření v oblasti kybernetické bezpečnosti bez značné finanční zátěže.

4. Možnosti financování

Nina Hoppmann, členka týmu ECCP

Na závěr se Nina Hoppmannová podělila o následující příklady možností financování:

1. Supporting competitiveness and innovation potential of SMEs; uzávěrka přihlášek je 7. listopadu 2023.
2. EIT Manufacturing: Empowering SMEs Call; uzávěrka přihlášek je 11. prosince2023.
3. Možnosti pro MSP: Výzvy Euroclusters jsou dostupné na European Cluster Collaboration Platform.
4. Pozvánka na C2Labs.