Účastníci odborné konference o NIS2 radí, jak zvládnout největší změny v kyberbezpečnosti za poslední léta. Klíčem je spolupráce a edukace

15.11.2023 - Mariana Pohlová | PROTEXT

Konferenci zahájil Petr Loužecký, ředitel úseku Algotech Cloud, GDPR a Kybernetická bezpečnost, který zároveň celou konferencí provázel.

Společnost Algotech je dlouhodobým partnerem a poskytovatelem služeb z oblasti business komunikací, podnikových systémů včetně vývoje na zakázku a v neposlední řadě je už více než 11 let provozovatelem cloudu specializovaného na dedikovaná řešení, bezpečnost a služby podpory. Prezentace byla zaměřena na využití cloudových služeb v rámci implementace NIS2, a to od zálohování přes řešení tzv. Disaster Recovery až po služby trvalého dohledu, včetně SOC či provozu aplikací spojených s bezpečností, např. log managementu LogMan.io, za nímž stojí další z partnerů konference.

Česká technologická a vývojářská společnost TeskaLabs se dlouhodobě specializuje na sofistikované produkty pro zajištění kybernetické bezpečnosti. V rámci konference vyzdvihla spoluzakladatelka, spolumajitelka a COO TeskaLabs Vladimíra Tesková roli moderního log managementu, který slouží ke sběru, archivaci a analýze logů. „Signature“ produkt TeskaLabs, LogMan.io, pomáhá rychle odhalit a analyzovat kybernetické hrozby i provozní incidenty a podává tak ucelený přehled o dění v IT infrastruktuře. Analýza dat v reálném čase nabízí prostor pro okamžitou reakci a nezměnitelně uložená data poskytují spolehlivý záznam incidentu pro účely vyšetření události a následné prevence. Důležitý je rovněž soulad s legislativou – implementací LogMan.io splňuje daný subjekt požadavky NIS2, ZoKB č.181/2014 Sb., VoKB č. 82/2018 Sb. nebo ČSN ISO 27001:2013.

Téměř výhradně otázkám NIS2 se pak věnoval Stanislav Simadl, Executive Director v MyCom Solutions. V obecné rovině zmínil odvětví, kterých se budou nová nařízení týkat, časový harmonogram související s národní legislativou nebo rozdělení úrovní povinností. Nastínil také vybraná organizační opatření, ať už jde o řízení dodavatelů, bezpečnostní role, audit kybernetické bezpečnosti nebo povinnosti top managementu. Stranou zájmu nezůstala ani technická opatření typu fyzická a síťová bezpečnost, centralizace identit uživatelů, antivirová ochrana, kryptografie, SIEM apod. nebo ostatní povinnosti (samoposouzení, registrace na NÚKIB, hlášení kyberbezpečnostních incidentů, bezpečnostní audit aj.). Samozřejmě se dotkl i otázky sankcí, které se mohou pohybovat v řádu desítek tisíc Kč za nedostatky až stamiliónů Kč za nedodržení povinností, případně i v podobě pozastavení výkonu řídicí funkce.

Michal Haas, Channel Business Developer ve společnosti ESET, se zaměřil na to, jak se technické požadavky v rámci NIS2 potkávají se statistikami společnosti ESET a podtrhují důležitost jejich řešení. Představil útok od různých vektorů infiltrace přes způsoby kompromitace uživatelských účtů až po jejich zneužití pro "nepozorovaný" průzkum sítě. Poukázal také na samotné zmocnění sítě za pomoci legitimních systémových nástrojů či použití různých variant malwaru. Účastníky seznámil také s použitím technologií pro ochranu různých komunikačních nástrojů, dvoufaktorovou autentizací pro ověření identity uživatele a s rozdíly mezi AV a EDR technologií včetně jejich hodnocení v rámci posledního testu EPR 2023 od společnosti AV-Comparatives.

Problematice SOC (Security Operation Center), tedy dohledové kyberbezpečnostní službě, se věnoval Jan Kozák, Presale Technical Specialist ze společnosti Axenta. V první části prezentace zmínil nejčastější cíle kyberbezpečnostních incidentů, mezi něž patří oblast vědy, výzkumu a vzdělávání, státní správy, armády, komunikace i zdravotnictví. Za těmito incidenty stojí ve 40 % hackerský útok, zatímco interní zaměstnanec je překvapivě viníkem v celých 60 % případů. Častým laickým omylem je představa, že stačí 1 klik a celá infrastruktura je jako mávnutím kouzelného proutku zavirovaná. Ve skutečnosti trvá 3-6 měsíců, než dojde k zahájení útoku, protože útočník se poměrně dlouhou dobu „rozhlíží" a hledá ta nejzranitelnější místa v systému. A právě tady nastupuje SOC 2.0, který představuje ucelené řešení, zodpovídající za identifikaci, analýzu i nahlášení bezpečnostních incidentů. Je tvořen moderními technologiemi i týmy specialistů a je schopen získávat informace z nejrůznějších zdrojů, ať už jde o antivirové programy či log management.

Roman Jiráček, Senior Account & Vendor Manager ze společnosti COMGUARD, se zaměřil na profesionální IT služby v souvislosti s požadavky NIS2 a třemi pilíři kybernetické bezpečnosti – technologiemi, informacemi a lidskými zdroji. V rámci IT security jde např. o analýzu zranitelností, penetrační testování s cílem odhalit bezpečnostní mezery firemní infrastruktury či doporučení nápravných opatření, bezpečnostní audity, phishingové kampaně k testování zaměstnanců nebo kurzy a školení. Účastníky seznámil i s virtuálním bezpečnostním analytikem pojmenovaným ThreatGuard. Jde o permanentně dostupnou, aktuální a strukturovanou databázi hrozeb a opatření.

Martin Wožniak, Head of Enterprise Sales & Business Development ve společnosti Whalebone, představil případové studie a modelové příklady využití produktu Whalebone, který řeší bezpečnost prostřednictvím DNS služby, kde blokuje škodlivý provoz a zamezí přístupu uživatelů ke škodlivým doménám. Firmy tím získávají plnou kontrolu nad DNS i neocenitelná data o své síti, a navíc i ochranu identity.

Firmy v Evropě budou muset v dohledné době řešit hned několik regulací a zákonů, které přinesou spoustu nových požadavků také pro náboráře a HR oddělení. O návod, jak se nezamotat do komplikovaných procesů, zejména při globálním náboru a čím dál častější remote práci, jak si vybrat spolehlivého partnera a dodavatele nebo jakým způsobem ověřit soulad s regulatorními požadavky se s účastníky podělil Petr Moroz, CEO startupu Scaut.com, který je středoevropským průkopníkem screeningu kandidátů v náboru a v posledních letech se se svým týmem věnuje vývoji technologií umožňujících efektivně bojovat proti neetickému využití AI v náboru zaměstnanců.

Závěr:

Konference představila novou odbornou platformu pro sdílení informací, zkušeností a názorů mezi odborníky z oblasti kybernetické bezpečnosti, zástupci firem a organizací podléhajících směrnici NIS2 a dalšími zájemci. Účastníci se dozvěděli o novinkách souvisejících s NIS2 a ZoKB, o povinnostech a výzvách s nimi spojených i o praktických zkušenostech z implementace požadavků. Seznámili se také s trendy a technologiemi v oblasti kybernetické bezpečnosti, které jim mohou pomoci zlepšit ochranu jejich systémů a služeb. Konference také ukázala, že spolupráce a edukace odborné i široké veřejnosti v oblasti kybernetické bezpečnosti je smysluplná a je třeba v podobných iniciativách pokračovat. Firmy a instituce z různých sektorů, které spojuje připravovaná směrnice NIS2, si dobře uvědomují důležitost sdílení znalostí a zkušeností. Vzájemná komunikace a kooperace jsou klíčové pro efektivní reakci na kybernetické hrozby a pro posilování odolnosti IT systémů. Organizátoři i partneři akce se shodli, že je potřeba udržovat dialog a výměnu informací mezi všemi zúčastněnými stranami, aby bylo možné čelit stále se měnícím a zvyšujícím se nárokům na kybernetickou bezpečnost – nejen v souvislosti s NIS2.

TeskaLabs

Technologická společnost TeskaLabs se dlouhodobě zabývá vývojem pokročilých softwarových produktů pro kybernetickou bezpečnost, jako jsou SIEM, Logmanagement a PKI řešení kybernetické bezpečnosti, které pomáhají firmám plnit vysoké bezpečnostní standardy v této oblasti.

Firmu založili Aleš Teska a Vladimíra Tesková v roce 2014. Oba už v tu dobu měli za sebou i další úspěšné společné projekty, mj. systém pro mobilní operátory, který monitoruje kvalitu služeb, nebo online nástroj projektového managementu.

Z původního ostře sledovaného startupu nabízejícího řešení pro zabezpečení mobilních aplikací a bezpečné připojení mobilních zařízení do firemních sítí se postupem času stala renomovaná technologická společnost v oblasti kybernetické bezpečnosti.

Velký podíl na tom mělo nejen přestěhování do Londýna, ale také účast v náročném programu prestižního globálního akcelerátoru TechStars, v němž byl TeskaLabs prvním českým startupem. Díky tomu si TeskaLabs vybrala britská pobočka firmy Cisco do svého programu podpory začínajících technologických firem.

Její služby a bezpečnostní řešení využívají firmy a instituce napříč odvětvími – např. O2, IKEM, TV Nova, TV Prima, Linet, AXA, Heureka, MPSV, Jablotron, Innogy, Axenta aj.

TeskaLabs je strategickým partnerem O2 Czech Republic a Cisco Solution Partner.

Firma má pobočky v Praze a Londýně.

Další informace na logman.io, www.teskalabs.com, na FCB, X nebo LinkedIn.

http://www.ceskenoviny.cz/tiskove/zpravy/ucastnici-odborne-konference-o-nis2-radi-jak-zvladnout-nejvetsi-zmeny-v-kyberbezpecnosti-za-posledni-leta-klicem-je-spoluprace-a-edukace/2440856