Kybernetická bezpečnost není pouze ochrana informací

MIROSLAV NEČAS

V roce 2017 jsme všichni implementovali SIEM systémy a zaváděli SOC. Loňský rok jsme horečně sháněli pověřence a prováděli GDPR audity. V roce 2019 bude hlavním tématem problematika řízení dodavatelského řetězce. Aktuální kauza kolem Huawei a ZTE je pouze první vlaštovkou z hejna.

Dlouhou dobu byla stěžejním úkolem kybernetické bezpečnosti ochrana informací. O únicích informací stále čítáme v médiích, přestože se dozvíme jen o zlomku z nich. Díky GDPR jsme v ochraně informací udělali krok kupředu. Firmy i státní organizace se začaly zajímat o to, kde mají citlivé informace a osobní údaje, jaká jsou s nimi spojená rizika, a začaly podnikat kroky k jejich zabezpečení. Mnozí si již uvědomili, že osobní údaje a citlivé informace se nacházejí i v šedých datech, a analýza obsahu šedých dat se stala nedílnou součástí analýzy informačního majetku organizace.

Bezpečnostní incidenty se však netýkají pouze informační bezpečnosti. Jsou zde kybernetická kriminalita, konkurenční boj, hacktivismus či jinak motivované útoky na výrobní zařízení nebo infrastrukturu. Dobře nastavené detekční systémy (SIEM, NetFlow, DLP, Endpoint Security atd.) zvyšují šanci zachytit podezřelé bezpečnostní události různého druhu. Ale bohužel často produkují tolik falešných poplachů, že není v lidských silách detekované události zpracovat a odhalit skutečné incidenty. Tisíce alarmů mají kvůli zahlcení obsluhy nulový efekt. Různé systémy zpravidla fungují nezávisle na sobě, a i když jsou bezpečnostní události sbírány do SIEM systému, často chybí širší kontext. Třeba informace o procesním a ekonomickém fungování organizace, údaje ze systému docházky či informace o aktuálních hrozbách a útocích z otevřených zdrojů. A tak lze jen stěží vyhodnocovat bezpečnostní události v širším kontextu, rozpoznat závažné incidenty a vyhodnocovat jejich dopady na organizaci. Kontext je rovněž zcela nezbytný pro zajištění důkazů a vyvození konkrétní odpovědnosti, pro návrh nápravných opatření a modelování dopadů kybernetických incidentů na chod organizace a kontinuitu provozu.

Jak souvisí řízení dodavatelského řetězce (supply chain management) s kybernetickou bezpečností?

Kauza kolem Huawei a ZTE mimo jiné ukázala, že každá technologie má zranitelnosti a každý dodavatel je vázán zákony mateřské země či může být napojen na rizikové subjekty. Tento problém se netýká pouze dodávané technologie. Dnes je běžné, že systémy pro řízení výroby jsou přímo integrovány se systémy dodavatelů či odběratelů. Vyžaduje to například nutnost zajištění kontinuální výroby při minimalizaci skladových zásob. Odhadem až 20 % firem nemá přehled o tom, s kým sdílí svá data. Ani zde problém řízení dodavatelského řetězce nekončí. Kvůli nedostatku lidských zdrojů je často řada činností outsourcována. Do infrastruktury firmy se díky tomu dostávají externisté, zaměstnanci dodavatelů a jejich subdodavatelů… Víte že až 70 % kybernetických útoků přichází ze sítí třetích, „důvěryhodných“ stran? Odhaduje se, že 63 % úniků informací mají na svědomí lidé. Rizika spojená s dodavatelským řetězcem se proto netýkají jen technologie. Nutností je prověřovat externí firmy a osoby, které jejich jménem vstupují do infrastruktury organizace. Co lze prověřit? Například napojení dodavatelských firem na konkurenci či rizikové subjekty, důvěryhodnost společností a zejména jejich bezpečnostní vyspělost a známé zranitelnosti dodávané technologie.

Tovek ARMS umožňuje kombinovat údaje o informační bezpečnosti, kybernetických útocích a dodavatelském řetězci do názorných manažerských přehledů. Přispívá k tomu, aby byly bezpečnostní incidenty zachyceny dříve a byly minimalizovány jejich dopady na provoz, reputaci a konkurenceschopnost.

Autor je Business development manager ve společnosti TOVEK.

Máte svého CCO?

Kybernetická bezpečnost, ochrana osobních údajů, řízení rizik a řízení dodavatelského řetězce jsou v organizaci často samostatnými agendami spadajícími do kompetence CIO, CEO, CTO, CFO… Ukazuje se, že je to nejen neefektivní, ale že to může být přímo nebezpečné. Protože schází ucelený pohled na kybernetickou bezpečnost a řada signálů o probíhajících incidentech uniká pozornosti. Vyspělé organizace proto zavádějí pozici CCO (Chief Cybercrime Officer) či využívají poradce boardu pro kybernetickou bezpečnost. Nejde o IT pozici, i když určité ICT kompetence jsou nezbytné. Větší důraz je kladen na znalost byznysu, analytické myšlení a zkušenosti v oblasti bezpečnosti. CCO nenahrazuje SOC či GDPR pověřence, ale zastřešuje vyšetřování incidentů. K tomu musí mít adekvátní nástroje, které umožní efektivně analyzovat výstupy z různorodých interních systémů a relevantní informace z externích zdrojů. CCO mimo jiné hlídá hlídače – IT administrátory, kybernetické experty či auditory.

Tovek ARMS – zbraň v boji s kybernetickým zločinem

Analytický, rešeršní a monitorovací systém (ARMS) je prověřen lety nasazení v oblasti vyšetřování organizované kriminality, finančních podvodů, bezpečnostních rizik a kybernetických hrozeb. Využívají ho státní i soukromé organizace v ČR i v zahraničí. Umožňuje konsolidovat informace ze SIEM systémů, monitoringu firem a osob, systémů řízení výroby a dalších systémů uvnitř i vně organizace, které obsahují informace relevantní pro vyšetřování bezpečnostních incidentů. ARMS umožňuje CCO z jednoho místa snadno dohledat informace o kontextu bezpečnostní události a rychle rozhodnout, zda jde o incident. Pokud ano, ARMS umožní shromáždit důkazy potřebné pro vyvození interní odpovědnosti, případně pro podání trestního oznámení.