HN obsah rozhoduje

KYBERNETICKÁ BEZPEČNOSŤ

PIATOK – NEDEĽA
27. – 29. MÁJA 2022

Partneri špeciálnej prílohy:

ALISON

ALITER TECHNOLOGIES

Nechajte ich pohrať sa. Sú to bezpečáci

Kybernetické cvičenia a hry sú skvelou príležitosťou pripraviť sa na neočakávané udalosti pre organizácie aj profesionálov. SNÍMKA: DREAMSTIME

TÉMA

Kyberzločinecké gangy sú vytrvalé, inovatívne a vyznávajú „beh na dlhé trate“. Obrancovia musia robiť to isté.

Stouto myšlienkou úspešne trénuje profesionálov a prednáša po celom svete Joseph Carson, etický hacker s viac ako 25-ročnými skúsenosťami.

Na rok 2022 predpovedá Joseph Carson vzostup modelu, ktorý opisuje ako ransomware-as-a-subscription. Čiže vydierači budú žiadať „výpalné“ za to, že nenapadnú organizáciu.

Podobným výpalným je vyhrážka „nezaplatíš, zaútočíme hrubou silou“. V minulom roku sa s takými hrozbami stretlo aj viacero organizácií na Slovensku.

Najčastejší útok

Ak teda môže zamestnanec čítať e-maily, otvárať dokumenty, browsovať na internete, klikať na odkazy alebo pripojiť zariadenie USB, môže spôsobiť kybernetický útok.

Útočníci tak dokážu zničiť veľkú organizáciu len tým, že sa zamerajú na jedného zamestnanca. Identifikáciu ľahko urobia na sociálnych sieťach, prihlasovacie údaje zamestnanca si zakúpia na dark webe.

Pomocou týchto informácií je ľahké vytvoriť phishingový e-mail, ktorý oklame aspoň jednu osobu. Obrana sa prelomí a škodlivý kód prenikne do siete.

Ako u nás doma?

Phishing zostáva najrozšírenejším a najničivejším útokom aj na Slovensku. Medzi zneužívané značky v minulom roku patrili pošta, dopravcovia, banky, ale aj Finančná správa. Okrem toho vás mohli prekliky doviesť najčastejšie na falošné chatovacie aplikácie či inzertné portály.

Ako potvrdzuje štatistika Národného centra kybernetickej bezpečnosti SK-CERT, najčastejšie hlásenými a detegovanými incidentmi za minulý rok na Slovensku bolo získavanie informácií. Takže nepozorní či naivní používatelia prispeli k tomu, že počet incidentov stúpol na vyše 400-tisíc. Cieľom bolo najmä získavanie bankových údajov.

Je dobré to vedieť

Tradičné technologické riešenia už nezastavia vysoko organizované skupiny kybernetického zločinu. Bežné antivírusové programy často nedokážu zabrániť a odhaliť útoky kvôli jedinečným a rýchlo sa meniacim variantom škodlivého kódu.

Počítače, tablety a smartfóny – čiže koncové body zároveň poskytujú čoraz viac príležitostí na prienik do IT prostredia a prístup k citlivým informáciám.

Bezpečnosť sa takto neustále vyvíja, takže takto dynamicky by sa k nej malo aj pristupovať. A to kladie vysoké nároky na to, ako vzdelávanie a osvetu robiť atraktívne.

Na sieťach sme nahí

Stojíme proti útočníkom zručným v podsúvaní nepravdivých informácií, ktoré klasické nástroje už nedokážu spoľahlivo odhaliť. Pokročilé útočné techniky využívajú zber informácií z verejne dostupných zdrojov a nekonečnou studnicou sú sociálne siete.

Polovica dospelých Američanov sa obáva množstva svojich osobných informácií, ktoré sú online. Takmer rovnaký podiel (47 percent) pripúšťa, že nerozumejú tomu, čo sa robí s ich zhromaždenými údajmi.

Uvádza to autor knihy Dilema sociálnych médií Michael Goedeker, doktorand v oblasti kybernetickej špionáže. Vydal ju v januári s podnadpisom Odhaľovanie nástrah a rizík skrývajúcich sa za pôvabom používania sociálnych médií. O používaní sociálnych médií hovorí ako „o pohybe na mínovom poli“.

Výzva každý deň

Výskum Michaela Goedekera sa zameriava na globálne kybernetické hrozby, ale koncovka je pozoruhodná. „Mojím cieľom je, aby boli bezpečnostné produkty, procesy, riešenia a obrana proti kybernetickým hrozbám čo najjednoduchšie pochopiteľné a implementovateľné,“ vysvetľuje. A tak publikuje v médiách, píše knihy a na jeho prednášky sa čaká mesiace. V súčasnosti vidí akútne úlohy kybernetickej bezpečnosti v ochrane ľudí a dodávateľského reťazca a znížení závislosti od sociálnych sietí.

> Účastníci často nepotrebujú našu správu so zisteniami, lebo na väčšinu prídu už počas cvičenia sami.
>
> **Zuzana Duračinská,** bezpečnostná odborníčka SecurityScorecard

Vo vzdelávaní prízvukuje, aké dôležité je duševné zdravie ľudí pri obrane pred propagandou a dezinformačnými útokmi. Ľudia, ktorí sú v spoločnosti a práci doceňovaní, sa vedia lepšie brániť. „O tom, ako sociálne siete ovplyvňujú zdravie, sa v súčasnosti ešte stále dostatočne nediskutuje ani neučí.“

Aj Michael Goedeker upozorňuje na to, že malé a stredné podniky a verejný sektor sú dnes atakované viac ako kedykoľvek predtým. Majú veľa slabých článkov a zároveň sú životne dôležité pre verejnosť aj stabilitu krajiny.

Na veľkosti nezáleží

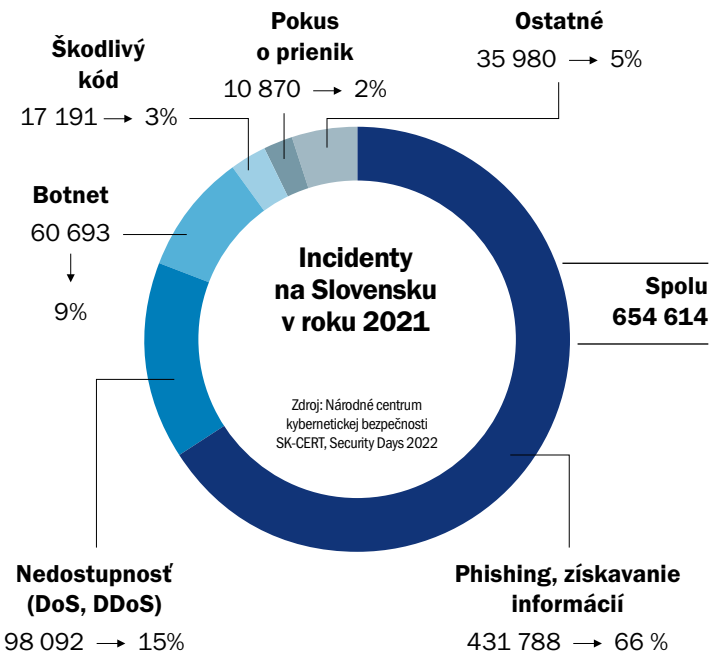
Hrozby majú rôznu povahu a veľkosť firmy v tomto prípade nehrá dôležitú úlohu. Zvnútra ohrozuje organizácie najčastejšie nevedomosť zamestnancov a „single point of failure“ – osoba, na ktorej stojí a zároveň padá základná obrana.

Ako ďalšie ohrozenia vymenúva bezpečnostná odborníčka Zuzana Duračinská zo spoločnosti SecurityScorecard nedostatočné interné riadenie softvéru tretích strán a neuvedomenie si tohto rizika.

Ako zabaviť riaditeľov

Každá organizácia by sa preto mala otestovať, ako je pripravená čeliť incidentu. Ideálnym nástrojom je kybernetické cvičenie.

Počas dvojhodinového cvičenia sa rýchlo odhalia slabé, ale aj silné stránky pripravenosti organizácie. Zároveň je to ideálna príležitosť pre manažment, aby porozumel aktuálnym hrozbám a ich reálnemu dosahu.



Cvičenie testuje spoluprácu tímu aj krízové plány „na papieri“ a veľmi rýchlo sa príde na to, ktoré časti potrebujú zlepšenie alebo sú v praxi nevykonateľné.

Cvičeniu neujde nikto

Manažérske cvičenia – tabletop sú paradoxne určené najmä pre iné oddelenie ako IT alebo bezpečnosť. Vedie ich profesionál kybernetickej bezpečnosti a účastníci môžu byť všetci vedúci pracovníci alebo vertikálne celé oddelenie.

„Zaujímavé je, že účastníci často nepotrebujú našu správu so zisteniami, lebo na väčšinu prídu už počas cvičenia sami,“ opisuje zážitky Zuzana Duračinská. Cieľ je dosiahnutý, ak si potrebu kyberbezpečnosti uvedomí top manažment a organizácie naštartujú zmeny.

Hacking gamification

Útočníci totiž stále hľadajú najlacnejší, najrýchlejší a najtajnejší spôsob, ako dosiahnuť cieľ.

„Zostať v obraze a naučiť sa hackerské techniky je jedným z najlepších spôsobov, ako vedieť brániť organizáciu pred kybernetickými útokmi,“ hovorí Joseph Carson. Už roky trénuje zručnosti a oboznamuje profesionálov s novými zraniteľnosťami. V priamom prenose ukazuje techniky, ako útočník prešiel od nuly k úplnej kompromitácii správcu domény a potom k zničujúcemu incidentu.

Vyzbrojení znalosťami si potom účastníci skúšajú etický hack, aby otestovali obranyschopnosť vlastnej organizácie. Bezpečnostný tím by mal takto pochopiť hackerské techniky, penetračné testy aj reakcie na incidenty.

Spoločnosti podieľajúce sa na obsahu špeciálnej prílohy

auditori.it · eset · Progress | Flowmon · MICRO FOCUS · Qubit · SOITRON · SK CERT NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

Trendy: Ani jeden rok nie je rovnaký

ANKETA

Prestížne stredoeurópske podujatie Qubit konferencia vytvára inšpiratívny priestor pre bezpečnostných profesionálov. Pýtame sa ich: Aký trend či fenomén vás v ostatnej dobe zaujal?

Rastislav Janota, riaditeľ
Národné centrum kybernetickej bezpečnosti SK-CERT

Na svetovej úrovni vidím veľký nárast škodlivej aktivity štátnych hráčov, a to nielen Ruska. A spolu s tým rast aktivity aktivistických skupín často silno usmerňovaný niektorými štátmi. A zároveň (ale len v zahraničí) výrazný nárast pozornosti, ktorú vlády venujú kybernetickej bezpečnosti a odolnosti. Najmä na úrovni masívneho nárastu investícií do kybernetickej bezpečnosti zo štátnych prostriedkov. Na Slovensku je trend opačný.

Karel Řehka, riaditeľ
Národní úřad pro kybernetickou a informační bezpečnost

Za všeobecnú a globálnu výzvu dneška aj dohľadnej budúcnosti považujem bezpečnosť dodávateľských reťazcov a strategickú závislosť od nedôveryhodných dodávateľov technológií. Ak si môžeme zobrať nejaké ponaučenie z dnešnej bezpečnostnej krízy v Európe, tak je to nepodceňovať strategické závislosti od režimov, ktoré nezdieľajú naše hodnoty.

Katarína Rolná, riaditeľka Odboru bezpečnosti a BCM
Tatra banka

Hlavný negatívny trend súčasnosti je nárast počtu a zvýšená sofistikovanosť kybernetických útokov. Pravidelne evidujeme podvodné vlny, ktorých základným stavebným kameňom sú falošné e-maily, esemesky alebo telefónne hovory. Najmä správy a telefonáty spôsobujú pokročilou úrovňou klamlivých prvkov klientom veľké problémy.

Ján Ščamba, riaditeľ globálneho centra kybernetickej bezpečnosti
Siemens Healthineers

Pri ochrane aktív sa začína stierať rozdiel medzi fyzickou a kybernetickou bezpečnosťou a v blízkom období môžeme očakávať zlučovanie týchto kompetencií. Nové hrozby sú oveľa sofistikovanejšie ako technologické kapacity aktuálnych cybersecurity riešení. Na to, aby tieto hrozby zodpovední pracovníci boli schopní adresovať, musia mať jasne definovanú stratégiu manažovania rizík.

Ján Grujbár, generálny riaditeľ
Aliter Technologies

Zaujala ma opätovne obnovená diskusia o vychyľovaní rovnováhy medzi bezpečnosťou a súkromím. Nástroje a mechanizmy, ktoré majú potenciál slúžiť na boj proti rôznym formám kriminality, so sebou nesú značné bezpečnostné riziká. Týkajú sa nielen možnosti zneužitia kybernetickými útočníkmi, ale aj súkromia každého z nás.

Andrej Žucha, generálny riaditeľ
ALISON Slovakia

Máločo v našej profesii za ostatné obdobie ma tak potešilo, ako hráči v originálnej slovenskej CyberGame. Lepšie povedané – hráčky. Pani na rodičovskej dovolenke sadla ku kompu, začala riešiť bezpečnostné úlohy, ktoré napísali profesionáli z SK-CERT, a teraz ju čaká exkurzia vo svetovom laboratóriu. Najmladšia hráčka Katka má 14 rokov. Moja dôvera v budúcnosť slovenskej kybernetickej bezpečnosti pookriala.

Tatiana Valentová, expertka na ochranu osobných údajov
Algger, s. r. o.

NFT token ako technológia budúcnosti, s obrovským potenciálom pre bezpečné uchovávanie dát rôznych formátov. Jeho potenciál zastreli obchodníci s umením, čím sa pre širšiu verejnosť stal synonymom obchodovania s umením. Jeho skutočný potenciál poskytuje bezpečný, jedinečný a nezameniteľný spôsob uchovávania a prístupu k dátam v digitálnom svete. Technológia, ktorá čaká na svoje skutočné využitie.

Marián Klačo, vedúci oddelenia bezpečnosť informácií
Volkswagen Slovakia

Narastá legislatívny tlak na dôraznejšiu ochranu pred kyberhrozbami, napríklad v súvislosti s prichádzajúcou Európskou NIS2 direktívou. Zároveň vidíme nárast počtu sofistikovaných kyberútokov voči kritickej infraštruktúre, akými boli aj Industroyer2, Incontroller. Teší ma, že na pozadí týchto udalostí sa zvyšuje publicita tém kyberbezpečnosti a dôraznejšie sa uplatňujú základné praktiky ochrany pred hrozbami, akými sú odkrývanie zraniteľností a ich záplatanie.

Roman Čupka, hlavný konzultant
Progress | Flowmon a CEO Synapsa Networks

Vojna ukazuje, ako je kybernetický priestor úzko zviazaný s každodenným životom a priamo ovplyvňuje konvenčné vedenie „špeciálnej operácie“. Napríklad neúspešné pokusy o odstavenie Starlinku, ktorý umožňuje Ukrajine internetové pripojenie, či tlak hackerov skupiny Anonymous na odsun globálnych firiem z Ruskej federácie. Úniky dát a zdieľanie informácií na Telegrame a Twitteri sú signifikantným zdrojom celej škály hacktivizmu v tejto hybridnej vojne.

Andrej Mišura, partner
auditori.it

Pandémia a vojna na Ukrajine posunuli vnímanie kybernetickej bezpečnosti z odborných kruhov do každodenného života. Sily profesionálov a dobrovoľníkov z celého sveta sa spojili na obranu kritickej infraštruktúry. Žijeme v bezprecedentných časoch, keď sa napĺňajú slová nás „bezpečákov“ a bezpečnosť sa stáva kľúčovou súčasťou nielen riadenia spoločností, ale aj nás všetkých.

Zuzana Duračinská, bezpečnostná špecialistka
SecurityScorecard

V kybernetickej bezpečnosti sa neustále učíme a neprejde rok, keď sa neobjaví nový útok alebo natoľko závažná zraniteľnosť, ktorá dokáže ochromiť tisícky zariadení po celom svete. K týmto už dnes „očakávaným“ sa pridala zložitá geopolitická situácia, ktorá zásadne premiešava karty na poli kybernetickej bezpečnosti.

Boris Mutina, špecialista na e-mailovú bezpečnosť
Excello, s. r. o.

Potešila pripravenosť poskytovateľov základných služieb, keďže ich denne preveruje súčasný konflikt premietnutý do digitálneho sveta. Snaha, najmä v súkromnom sektore, nevyšla nazmar. Naopak, mrzí nepripravenosť a neschopnosť efektívne bojovať proti hybridným hrozbám, nielen na národnej, ale i nadnárodnej úrovni. Je smutné, že sa potichu očakáva záchrana od veľkých firiem, ale legislatíva chýba.

Martin Lohnert, riaditeľ centra kybernetickej bezpečnosti
Void SOC Soitron

Na ľudskú nevedomosť či nepozornosť sa zameriava nová technika Browser-v-browseri. Má za cieľ vylákať od obete prihlasovacie údaje, keď útočníci na podvrhnutej stránke ponúknu Single sign-on (SSO) prihlasovacie okno do Googlu či facebookového účtu, s falošnými „bezpečnostnými“ prvkami. To môže napriek svojej jednoduchosti zmiasť aj skúsenejších používateľov. Odporúčame SSO na weboch tretích strán vôbec nevyužívať, respektíve byť pri nich mimoriadne obozretný.

Martin Florián, generálny riaditeľ sekcie kybernetickej bezpečnosti
MIRRI SR

Zaujal ma nárast povedomia a praktickej aplikácii Zero Trust princípu – ničomu neznámemu a nikomu neoverenému slepo nedôveruj, kým sa nepreukáže opak. Na ceste, ako aplikovať tento princíp, existuje mnoho argumentov a pravidiel. Ak prioritizujeme ich implementáciu, musíme poznať vzorce, ako útočníci najjednoduchšie a najčastejšie získavajú prístup k citlivým údajom. Súčasťou Zero Trust princípu je tak proaktívne znižovanie rizika kompromitácie identity používateľa.

Tibor Paulen, manažér informačnej bezpečnosti
Stredoslovenská distribučná

Rozmach sociálnych sietí, cloudových riešení, digitalizácia a práca z domu úplne menia definíciu problému a aj definíciu jeho riešenia. Do zvládania bezpečnostných hrozieb je potrebné zapájať čoraz viac subjektov. Kým donedávna na to stačili kolegovia z IT sami, teraz pribúdajú bežní používatelia, biznis partneri a zákazníci. A stávajú sa súčasťou problému a aj jeho riešenia.

Július Selecký, senior technický špecialista
ESET

Z rozhovorov s manažérmi vyplynulo, že napriek výrazne lepšej situácii s COVID-19 väčšina zamestnancov pracuje z domu. Zhruba pätina sa do kancelárie už nevráti.
Tieto zmeny v spôsobe, akým pracujeme, otvorilo trend takzvanej home office security. Vynucovanie prísnejších IT bezpečnostných noriem, povinné VPN, prihlasovanie pomocou dvojfaktorovej autentifikácie, phishing školenia či zabezpečenie pracovných staníc systémom rozšírenej detekcie a reakcie na hrozby XDR.

Marcela Zimová, riaditeľka informačnej bezpečnosti
Piano Software

Z pohľadu používateľa ma fascinuje rozmach primitívnych útokov, ako sú podvody pri predajoch, phishingové esemesky od bánk alebo telefonáty z „podpory“, snažiace sa získať prístup k zariadeniam. Preto je dôležité zvyšovať bezpečnostnú gramotnosť verejnosti.
Z profesijného hľadiska ma zaujali nedávne rozhodnutia európskych dozorných orgánov v oblasti ochrany údajov z hľadiska používania Google Analytics.

Timea Tomčová, odborníčka IT bezpečnosti
Vychodoslovenská Holding

Eskalácia konfliktu medzi Ruskom a Ukrajinou zintenzívnila rozsah a sofistikovanosť hrozieb aj v kybernetickom prostredí.
Ak by som mala byť konkrétnejšia a uviesť príklady hrozieb, ktoré určite stoja za zmienku, tak tu svoje miesto nájdu škodlivé kódy HermeticWiper, Hodur, Emotet a Industroyer2. Princípov, ako na aktuálne hrozby reagovať, je mnoho.
Nie každému novému trendu odporúčam podľahnúť.

Rastislav Beňo, manažér informačnej bezpečnosti
Mitsubishi Chemical Advanced Materials

Zásadnou a pre nás veľmi potešiteľnou zmenou je čoraz väčšia obozretnosť a angažovanosť našich zamestnancov pri posudzovaní rizík spojených s masívnym používaním informačných technológií.
Svedčí to o tom, že naše aktivity smerujúce k vzdelávaniu a osvete v oblasti informačnej bezpečnosti majú význam a začínajú prinášať svoje ovocie. Sme globálna spoločnosť so zamestnancami na všetkých kontinentoch a tento trend pozorujeme celosvetovo.

Štefan Mizerák, manažér oddelenia IT bezpečnosti
NN Životná poisťovňa

Jednoznačne trend využívania propagandy, dezinformácií a štátmi sponzorovaných kybernetických útokov na kritickú infraštruktúru a médiá, ale aj na bežné firmy, teda otvorená vojna v kyberpriestore medzi štátmi s obrovským rozpočtom. Posledné mesiace stavajú silu informácií, ich vplyv na ľudský život a dôležitosť ich ochrany do nového svetla – kyberpriestor je dnes nebezpečnejší než zvyčajne.

Anna Stehlíková, manažérka pre bezpečnostné licencie Čechy a Slovensko
Micro Focus

Je fascinujúce sledovať, ako sa aplikačné programové rozhranie – API – stáva rastúcim vektorom útokov v ostatných desaťročiach. Je to dôsledok prechodu k mikroslužbám, či už používaniu aplikácií alebo cloudových služieb. Zvládnuť efektívne bezpečnostné overovania pre toto rozhranie sa stáva čoraz väčšou výzvou.

Vlastimil Balog, manažér informačnej bezpečnosti
Diebold Nixdorf

Momentálne najväčšou výzvou v oblasti informačnej bezpečnosti je takzvaná retencia kvalifikovanej sily. Štandardne sa pohybuje v priemere dva – tri roky, a to je málo vzhľadom na narastajúci dopyt po projektoch informačnej bezpečnosti. Všetky organizácie by mali zavádzať retenčné programy, ktorých úlohou by malo byť udržať kľúčových ľudí čo najdlhšie.

Radovan Šulek, expert na bezpečnosť
Energotel

Rast množstva incidentov a legislatívne požiadavky vedú k prehĺbeniu dlhodobého nedostatku kvalifikovaných ľudí, čo pred nás stavia viacero výziev. Získať viditeľnosť, čo sa deje v systémoch, sieti a aplikáciách. Minimalizovať riziká kombináciou vlastných a outsourcovaných špecialistov a optimalizovať bezpečnostné nástroje, aby sme využili ich potenciál a minimalizovali počet zariadení, ktoré potrebujú našu starostlivosť.

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 27. – 29. MÁJA 2022

Spoľahlivé informácie sú otázka

Iba pár kilometrov od našich hraníc sledujeme, ako sa kybernetické hrozby stali skutočnosťou. Deň pred začiatkom vojny bol znefunkčnený satelit, ktorý využívala Ukrajina na komunikáciu. A zároveň jedným z prvých prejavov pomoci bola alternatívna komunikačná satelitná sieť. Nepochybne to opäť ukazuje, že rýchla a dôveryhodná komunikácia je kľúčová.

Kybernetické hrozby majú rôzne formy a rovnako aj ich dosahy sa prejavujú rôzne. Najčastejšie a najznámejšie sú DDoS útoky (distributed denial-of-service), kde ide o zámerné zahltenie komunikačného kanála. Takýto útok sa dnes dá objednať za pár drobných ako služba z internetu. Takáto zlomyseľnosť je však ľahko odhaliteľná a relatívne rýchlo odstránená.

Najzložitejšie a najnepríjemnejšie formy kybernetických útokov sa nesú v znamení nechcených „kukučích vajec“, ktoré môžu roky ležať zabudnuté v databázových systémoch, alebo sa prebudiť na základe nastavených podnetov, čo je prípad trójskeho koňa.

Väčšina týchto kybernetických aktivít má za úlohu vykonať zmenu, ktorú „obeť“ nečaká. Tým môže byť napríklad narušenie integrity dát, zámerná zámena informácií alebo poškodenie či znefunkčnenie komunikačného systému.

Aby sa eliminoval vplyv kybernetických útokov na dostupnosť a dôveryhodnosť informácií, využívajú sa alternatívne druhy komunikácie. Musia byť energeticky nezávislé, mobilné, s telekomunikačnou konektivitou a najvyššími parametrami kybernetickej odolnosti. Požiadavkami sú aj maximálna operatívnosť, variabilita komponentov a pohyb v teréne.

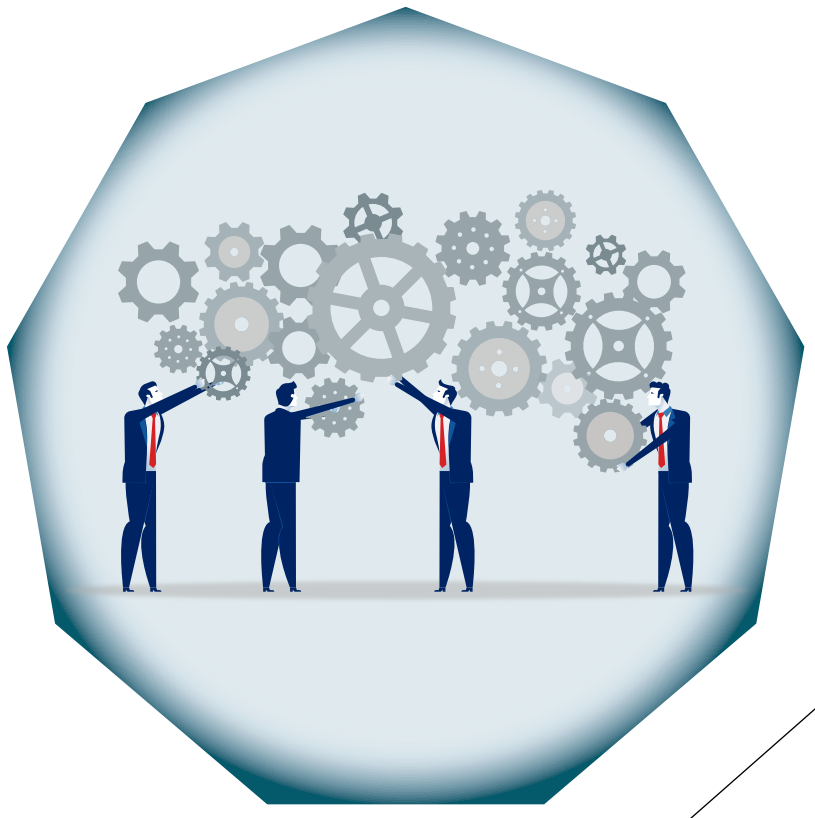
Na zabezpečenie spoľahlivej, dôveryhodnej a nerušenej komunikácie na malé a stredné vzdialenosti sa využívajú komunikačné a bezpilotné vzdušné prieskumné systémy. Dokážu prenášať hlas, obraz a dáta v základnej verzii niekoľko desiatok kilometrov a s ďalšími rozširujúcimi modulmi vždy o ďalšie desiatky.

Pozorovacie a komunikačné systémy sa prepájajú s operačným strediskom velenia a zároveň je možné operácie riadiť priamo z terénu.

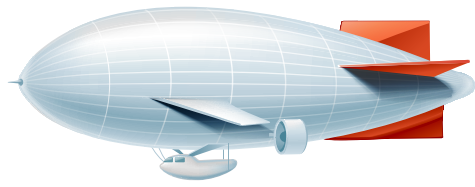
Alternatívne druhy komunikácie slúžia aj v prípade, ak nie je k dispozícii stála infraštruktúra alebo počas záchranných akcií a hromadných podujatí. Všade tam, kde je nevyhnutné chrániť dostupnosť a dôveryhodnosť informácií.

Imrich Petruf, riaditeľ divízie Špeciálnych systémov Aliter Technologies

Komunikačný a bezpilotný vzdušný prieskumný systém



upútaný dron – – virtuálny stožiar



monitorovacia vzducholoď

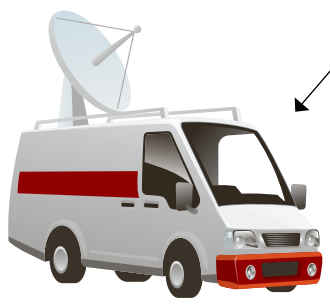
Tieto komponenty môžu niesť rôzne senzory, kamery pre vizuálne pozorovanie, rádiostanice, alebo bázové stanice na pokrytie GSM signálom.

pracovisko pre riadenie dronu a vzducholode

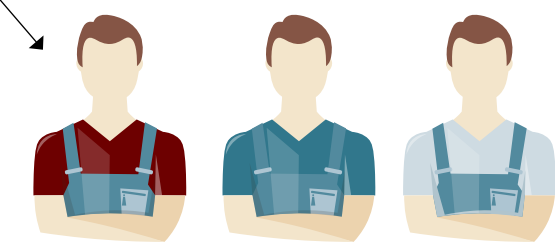
Komunikačný a bezpilotný vzdušný prieskumný systém je riadený z mobilného miesta riadenia.

Mobilné miesto riadenia sa skladá z vozidla s upútaným dronom – virtuálnym stožiarom s monitorovacou vzducholoďou

Vo vozidle sa nachádzajú pracoviská pre riadenie systémov. Trojčlennú posádku tvoria traja ľudia, operátor, pilot, ktorý dohliada na dron či vzducholoď a zaškolený obsluhujúci technik



vozidlo



trojčlenná posádka

PRIPOJENIE

Mobilné miesto riadenia je možné pripojiť k pracoviskám prenosovej infraštruktúry lokálnej siete, alebo na sieť internet, vrátane satelitného spojenia.

PRENOS INFORMÁCIÍ

Systém vytvára vlastnými rádiovými vlnami komunikačno-informačný kanál, zabezpečený prostriedkami šifrovej ochrany informácií. Tým vytvára dočasné bezpečné komunikačné prostredie, nezávislé od stavu stálej infraštruktúry. Údaje zo senzorov sa tak spoľahlivo prenášajú až ku koncovému používateľovi.

Globálny trh s kybernetickou bezpečnosťou v oblasti obrany

29,81
AMERICKÝCH DOLÁROV
v roku 2028

19,96
MILIÁRDY
amerických dolárov
v roku 2021

Zdroj: Fortune Business Insights.com

KOMENTÁR

Naše štyri roky s nariadením GDPR? Veľmi intenzívne

Denne vpúšťame do súkromia množstvo rôznych subjektov. Prístupom k odtlačku prsta pri mobiloch, osobnými fotografiami, udalosťami v kalendári, nákupnými preferenciami, lokalizačnými údajmi, surfovaním na internete či snímaním hlasu sprístupňujeme veľkú časť súkromného života „cudzím“ subjektom.

Májové výročie účinnosti Nariadenia na ochranu osobných údajov v členských štátoch EÚ je preto výborný dôvod, aby sme si to ešte viac uvedomovali.

Pred štyrmi rokmi išlo v prípade GDPR o celkom slušnú „evolúciu“, a to najmä s ohľadom na online biznis. Ako sa ukázalo v praxi, často nič nehovoriacej papierovej dokumentácii odzvonilo a nastal čas zamerať sa na reálnu ochranu osobných údajov.

Pozitívom GDPR je určite fakt, že dotknuté osoby, čiže my všetci, si výraznejšie uvedomujeme hodnotu svojich osobných údajov. Čoraz viac sa intenzívne stretávam s prípadmi, že dotknuté osoby si výrazne a vo veľkom rozsahu uplatňujú práva na ochranu osobných údajov v zmysle GDPR a celkom slušne si tieto inštitúty osvojili.

Rovnako ma zaujala aj aktivita Úradu na ochranu osobných údajov, ktorý sa za štyri roky výrazne posilnil nielen kvalitatívne, ale aj personálne. V neposlednom rade nie je zanedbateľná ani jeho rozsiahla rozhodovacia činnosť. Na viacerých kontrolách zo strany Úradu u našich klientov som bol svedkom toho, že kontrolné tímy dávali veľmi trefné otázky a dopyty, a mali k dispozícii aj kyberšpecialistov.

Preto v tomto smere zdôrazňujem, že proces súladu s GDPR je neustály a pri mnohých klientoch celkom dynamický. A bezpochyby vyžaduje permanentné konzultácie a podporu v oblasti spracúvania osobných údajov a zabezpečovania súladu s GDPR.

Osobne sa mi páči, že to nie je len statická legislatíva, ale akýsi súbor pravidiel a požiadaviek na zabezpečenie reálnej ochrany osobných údajov dotknutých osôb. A to vrátane rizík s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb.

Ako negatívum vnímam, že sa od počiatku účinnosti nariadenia sa objavili rôzni „experti“ na zabezpečovanie súladu prevádzkovateľov s GDPR. Často disponujú prevažne len všeobecnou papierovou akože bezpečnostnou dokumentáciou, ktorá absolútne nezabezpečuje súlad.

Neraz sme po takýchto pseudoexpertoch u klientov napravali tento stav a po vykonaní auditu bolo potrebné nastaviť a zaviesť celkom nové bezpečnostné a organizačné opatrenia. Žiaľ, aj po rokoch od účinnosti nariadenia je ich ešte veľa.

Súlad s požiadavkami nariadenia je stálym procesom preverovania a posudzovania zhody spracúvania osobných údajov prevádzkovateľmi s GDPR. Súčasne s tým, ako sledujeme vývoj legislatívy, technologický a technický progres sietí a informačných systémov a v neposlednom rade aj oprávnenia Úradu.

Aj po štyroch rokoch života s GDPR musím prisvedčiť, že v spracúvaní osobných údajov ma vždy niečo nové zaujme. Rozhodne to nie je niečo nalinajkované, statické alebo nemenné, ale je to ozaj živý proces.

Miroslav Chlipala
Advokátska kancelária Bukovinský & Chlipala