**Jak narody radzą sobie z globalnymi zagrożeniami cybernetycznymi?**

Ataki na infrastrukturę informacyjną i usługi internetowe mogą teraz zaszkodzić społeczeństwu w nowy i krytyczny sposób. Oszustwa internetowe i ataki hakerskie to tylko niektóre przykłady przestępstw komputerowych, które są codziennie popełniane na dużą skalę. Liczba cyberataków na światowe rządy i przedsiębiorstwa komercyjne stale rośnie pod względem częstotliwości i dotkliwości. Cyberbezpieczeństwo odgrywa kluczową rolę w ciągłym rozwoju technologii informatycznych, a także usług internetowych. Zwiększenie cyberbezpieczeństwa w celu ochrony krytycznej infrastruktury informatycznej ma zasadnicze znaczenie dla bezpieczeństwa i dobrobytu gospodarczego każdego narodu. Czynienie internetu bezpieczniejszym i ochrona użytkowników internetu stały się podstawą rozwoju nowych usług i polityki rządowej. Zgodnie z najnowszym kompleksowym badaniem dotyczącym cyberprzestępczości 2013 opublikowanym przez Biuro Narodów Zjednoczonych ds. Narkotyków i Przestępczości (UNODC), prawie połowa krajów biorących udział w badaniu przyjęła przepisy o ochronie danych, które określają wymagania dotyczące ochrony i wykorzystywania danych osobowych. Niektóre z tych systemów zawierają szczególne wymagania dla dostawców usług internetowych i innych dostawców łączności elektronicznej. W wielu krajach rozwiniętych obowiązują również przepisy wymagające od organizacji powiadamiania osób fizycznych i organów regulacyjnych o naruszeniach danych. Około 70% krajów, które udzieliły odpowiedzi zgłosiło, że strategie krajowe obejmowały elementy dotyczące podnoszenia świadomości, współpracy międzynarodowej i zdolności egzekwowania prawa. Chociaż krajowe możliwości, potrzeby i zagrożenia są różne, wiele krajów stoi w obliczu tych samych zagrożeń, takich jak zależność cybernetyczna, wymiana danych między krajami i zmiany w środowisku pracy. Aby zrozumieć znaczenie cyberbezpieczeństwa oraz elementy holistycznego i opartego na strategii krajowego programu cyberbezpieczeństwa, musimy najpierw rozpoznać kluczowe globalne zagrożenia.

**WPŁYW GLOBALNEGO CYBERRYZYKA**

Światowe Forum Ekonomiczne definiuje „globalne ryzyko" jako niepewne zdarzenie lub stan, który, jeśli wystąpi, może mieć znaczący negatywny wpływ na kilka krajów lub branż w ciągu najbliższych 10 lat. Globalne zagrożenia materializują się w nowy i nieoczekiwany sposób i stają się coraz bardziej nieuchronne, gdy ich konsekwencje dotrą do ludzi, instytucji i gospodarek. Brak zrozumienia i przeciwdziałania zagrożeniom związanym z technologią, przede wszystkim systemowym kaskadowym skutkom cyberzagrożeń lub awarii krytycznej infrastruktury informatycznej, może mieć daleko idące konsekwencje dla gospodarek krajowych, sektorów gospodarki i przedsiębiorstw globalnych. Przedsiębiorstwa, decydenci polityczni i społeczeństwo obywatelskie muszą znaleźć odpowiednie ramy, aby zaradzić poważnym zagrożeniom związanym z transformacją w kierunku bardziej zdigitalizowanej gospodarki. Według The Global Risks Report 2016, według jednego z szacunków, kraje europejskie, które nie reagują odpowiednio na zmiany technologiczne, mogą stracić 600 miliardów euro wartości dodanej w ciągu najbliższych 10 lat, co odpowiada około 10% europejskiej bazy przemysłowej. Poniżej przedstawiono globalne zagrożenia cybernetyczne zidentyfikowane przez Światowe Forum Ekonomiczne.

**Globalne zagrożenia cybernetyczne**

**Ryzyko cybernetyczne: Opis**

Niekorzystne konsekwencje postępu technologicznego : Zamierzone lub niezamierzone negatywne konsekwencje postępu technologicznego, takiego jak sztuczna inteligencja, geoinżynieria i biologia syntetyczna, powodujące szkody dla ludzi, środowiska i gospodarki.

Podział krytycznej infrastruktury i sieci informatycznych: Zależność cybernetyczna zwiększa podatność na awarie krytycznej infrastruktury informatycznej (np. Internetu, satelitów itp.) oraz sieci powodujących szerokie zakłócenia

Cyberataki na dużą skalę : cyberataki na dużą skalę lub złośliwe oprogramowanie powodujące duże szkody gospodarcze, napięcia geopolityczne lub powszechną utratę zaufania do Internetu.

Masowy incydent oszustwa/kradzieży danych : niewłaściwa eksploatacja prywatnych lub oficjalnych danych, która ma miejsce na niespotykaną dotąd skalę.

Zależność cybernetyczna: Naród zależy od funkcjonowania technologii informacyjno-komunikacyjnych oraz działania krytycznej infrastruktury informatycznej. Na przykład nasze interakcje, transport, komunikacja, handel i handel elektroniczny, usługi finansowe, usługi o znaczeniu krytycznym opierają się na poufności, integralności i dostępności informacji przepływających przez te infrastruktury. Jednak za tą rosnącą zależnością od cyberprzestrzeni kryją się nowe zagrożenia, które zagrażają gospodarce i bezpieczeństwu państwa. Wrażliwe dane, sieci i systemy, którym obecnie ufamy, mogą zostać naruszone lub uszkodzone, w taki sposób, że wykrywanie lub obrona może być trudne, co podważa nasze zaufanie do gospodarki opartej na sieci. Wraz ze wzrostem cyberzależności wynikające z tego połączenia i współzależność sprawiają, że infrastruktura krytyczna jest bardziej podatna na ataki. Niedawne badanie sugeruje, że technologie związane z Internetem, takie jak internet mobilny, automatyzacja pracy z wiedzą, IoT i technologia chmury, będą najbardziej destrukcyjne, generując jednocześnie największe korzyści ekonomiczne. Wraz ze wzrostem tempa innowacji rozprzestrzenianie się technologii jest nieuniknione i wymaga szybkiej adaptacji, takich jak modele biznesowe, procesy i ramy bezpieczeństwa. Według badań Światowego Forum Ekonomicznego cyberataki i związane z nimi incydenty od pewnego czasu wkraczają w światowy krajobraz zagrożeń jako jedno z najbardziej prawdopodobnych i potencjalnie najskuteczniejszych zagrożeń – w Ameryce Północnej cyberataki zajmują zdecydowanie najbardziej prawdopodobne ryzyko. Ponieważ mobilny Internet i IoT prowadzą do większej liczby połączeń między ludźmi i maszynami, cyberzależność jest uważana za znaczący globalny trend, zwiększający szanse na cyberataki z potencjalnymi skutkami kaskadowymi w całym cyberekosystemie. Ryzyko jednostki jest coraz bardziej powiązane z ryzykiem innych jednostek w połączonym środowisku. Światowe Forum Ekonomiczne sugeruje, że mobilny internet i połączenia maszyna-maszyna to dwa obszary, które są niedostatecznie chronione. Każde słabo zabezpieczone urządzenie podłączone do Internetu potencjalnie wpływa na bezpieczeństwo Internetu zarówno globalnie, jak i lokalnie.

Wymiana danych między krajami i interesariuszami: Dane zostały uznane za „ropę XXI wieku". W związku z tym potrzebne są przewidywalne ramy prawne, aby w pełni wykorzystać potencjał gospodarczy cyfryzacji, ponieważ stworzenie odpowiedniej infrastruktury prawnej jest integralnym elementem krajowej strategii cyberbezpieczeństwa. Na przykład zarządzanie krajowe należy uzupełnić funkcjonującymi międzynarodowymi ramami prawnymi w obszarach takich jak łańcuchy dostaw czy druk 3D. Według The Global Risks Report 2016, obecny system regulacyjny jest słabo rozwinięty i brakuje niezbędnej pewności prawnej w obszarach takich jak prywatność, przejrzystość, kontrola szyfrowania, wpływ systemów własności intelektualnej na dane przekraczające granice oraz wpływ danych zastrzeżonych na konkurencja. Ponadto fizyczna infrastruktura do wymiany danych, taka jak kable podmorskie, może również stać się celem w przypadku konfliktu międzynarodowego lub terroryzmu. Przyjęcie przez wszystkie kraje odpowiednich przepisów przeciwko nadużywaniu technologii informacyjno-komunikacyjnych przez przestępców, takich jak działania mające na celu naruszenie integralności krajowych krytycznych infrastruktur informatycznych, ma zasadnicze znaczenie dla osiągnięcia globalnego bezpieczeństwa cybernetycznego.

Zmiany w środowisku pracy: Dzięki nowym technologiom powstanie wiele nowych rodzajów miejsc pracy. W międzyczasie nastąpi wysiedlenie pracowników o niskich kwalifikacjach i robotników z powodu automatycznych i kontrolowanych przez IT procesów, ponieważ istniejące kategorie miejsc pracy zostaną skomputeryzowane. Amerykańskie Biuro Statystyki Pracy szacuje, że 47% pracowników w USA będzie miało duże prawdopodobieństwo, że ich praca zostanie zautomatyzowana do 2022 roku. Zwiększone wykorzystanie oprogramowania i interfejsów IT spowoduje wzrost popytu na architektów rozwiązań IT. Ponieważ wdrażanie robotów staje się coraz powszechniejsze, producenci będą musieli stworzyć nową rolę koordynatora robota, co spowoduje stworzenie dodatkowego miejsca pracy.

**Przykłady nowych rodzajów ról wynikających z Przemysłu 4.0**

**Naukowiec ds. danych przemysłowych:**

* Wyodrębnij i przygotuj dane, przeprowadzaj zaawansowane analizy i wykorzystuj ich wyniki do ulepszania produktów lub produkcji.

* Zrozum zarówno procesy produkcyjne, jak i systemy informatyczne oraz przetwórz silne umiejętności analizy przyczyn źródłowych, aby zidentyfikować korelacje i wyciągnąć wnioski.

**Koordynator robotów**

* Nadzoruj roboty na hali produkcyjnej i reaguj na awarie lub sygnały o błędach.

* Wykonuj zarówno rutynowe, jak i awaryjne zadania konserwacyjne i w razie potrzeby angażuj innych ekspertów.

Zmniejszy się zapotrzebowanie na pracowników wykonujących proste i powtarzalne zadania, ponieważ czynności te mogą być ustandaryzowane i wykonywane przez maszyny. Według Światowego Forum Ekonomicznego, ręczne zadania mogą być przejęte przez roboty, takie jak prowadzenie zapasów detalicznych online, opieka zdrowotna i diagnostyka oraz odprawianie gości hotelowych. Doświadczeni pracownicy wykonujący nierutynowe zadania poznawcze mogą zostać zastąpieni przez postępy w inteligentnych algorytmach. Przykłady miejsc pracy zastępowanych przez roboty obejmują:

• Operatorzy telefoniczni

• Fotografowanie pracowników procesu i operatorów maszyn przetwórczych

• Pracownicy usług pocztowych

• Technicy i pracownicy przygotowalni

• Pracownicy egzekwowania prawa parkingowego

• Czytniki liczników i mediów

• Spikerzy

• Pośrednicy biur podróży

Zmieniający się krajobraz zatrudnienia ma znaczące implikacje dla przedsiębiorstw przemysłowych, systemów edukacji i rządów, ponieważ cały system zatrudnienia wymaga ponownej oceny, aby ułatwić przechodzenie między różnymi rodzajami pracy. Oczekuje się, że umiejętności w zakresie STEM (nauka, technologia, inżynieria i matematyka) wzrosną w perspektywie średnioterminowej, przy przewidywanych długoterminowych potrzebach skupienia się na umiejętnościach takich jak kreatywność, rozwiązywanie problemów i inteligencja społeczna. Umożliwienie firmom przekwalifikowania ich siły roboczej, systemy edukacyjne w celu zlikwidowania luki w umiejętnościach

informatycznych oraz wzmocnienie wsparcia rządów będą miały kluczowe znaczenie dla realizacji obietnicy postępu technologicznego.

**PRZYKŁAD Z PRAWDZIWEGO ŚWIATA**

**Atak na ukraińską sieć energetyczną**

Cyberatak na zachodnioukraińskie firmy dystrybucyjne energii elektrycznej Prykarpattya Oblenergo i Kyiv Oblenergo 23 grudnia 2015 r. spowodował poważną awarię zasilania w ponad 50 podstacjach w sieciach dystrybucyjnych. Podobno w regionie wystąpiła kilkugodzinna przerwa w dostawie prądu, a wiele innych klientów i obszarów miało mniejsze przerwy w dostawach energii, dotykając ponad 220 000 konsumentów. Niektórzy obwiniali o atak wykorzystanie szkodliwego oprogramowania BlackEnergy po zidentyfikowaniu próbek w sieci. Co najmniej sześć miesięcy przed atakiem osoby atakujące wysłały do biur przedsiębiorstw energetycznych na Ukrainie wiadomości phishingowe zawierające złośliwe dokumenty Microsoft Office. Jednak złośliwe oprogramowanie prawdopodobnie nie było odpowiedzialne za otwarcie wyłączników automatycznych, które spowodowały awarię. Jest prawdopodobne, że złośliwe oprogramowanie umożliwiło atakującym zebranie danych uwierzytelniających, które umożliwiły im uzyskanie bezpośredniej zdalnej kontroli nad aspektami sieci, co z kolei umożliwiłoby im wywołanie awarii. Ten incydent na Ukrainie jest pierwszym potwierdzonym przypadkiem destrukcyjnego cyberataku na sieć elektryczną.

**ZNACZENIE CYBERBEZPIECZEŃSTWA**

Pojawienie się cyberprzestrzeni, wirtualnej domeny globalnej, wpłynęło na prawie każdy aspekt naszego życia. Dziedzina ta bardziej niż kiedykolwiek przekształca naszą gospodarkę i postawę bezpieczeństwa, tworząc możliwości dla innowacji i środki poprawy ogólnego dobrobytu obywateli. Tak jak w XIX wieku musieliśmy zabezpieczyć morza dla naszego narodowego bezpieczeństwa i dobrobytu, tak w XX wieku musieliśmy zabezpieczyć powietrze, tak w XXI wieku musimy także zabezpieczyć naszą pozycję w cyberprzestrzeni. Według wyników badania opinii kadry kierowniczej Światowego Forum Ekonomicznego (EOS), cyberatak jest postrzegany jako zagrożenie o największym zaniepokojeniu w ośmiu gospodarkach, w tym w Estonii, Niemczech, Japonii, Malezji, Holandii, Singapurze, Szwajcarii i Stanach Zjednoczonych. co najmniej dwa z tych krajów zostały niedawno zakłócone przez cyberataki: amerykańskie Biuro Zarządzania Personelem i Japoński Urząd Emerytalny. Według Światowego Forum Ekonomicznego, Global Risk Landscape 2016, cyberataki są jednym z zagrożeń o dużym wpływie i wysokim prawdopodobieństwie. Z około dwoma miliardami użytkowników na całym świecie Internet stał się istotną częścią naszego życia, dostarczając informacji i komunikacji na całym świecie. Jednak cyberprzestrzeń jest idealnym miejscem dla przestępców, ponieważ mogą pozostać anonimowi i uzyskać dostęp do wszelkich form danych osobowych. Cyberprzestępczość, pojawiająca się forma tradycyjnej przestępczości, jest jednym z najszybciej rosnących zagrożeń. Najczęstszą formą cyberprzestępczości są przestępstwa związane z tożsamością, do których dochodzi poprzez phishing, złośliwe oprogramowanie i hakowanie. Internet stał się także miejscem przestępstw związanych z prawami autorskimi oraz prawa własności intelektualnej i przestępstwa, takie jak pornografia dziecięca i materiały związane z nadużyciami. Cyberprzestępczość stała się łatwiejsza wraz z postępem technologicznym, którego sprawcy nie potrzebują już wielkich umiejętności ani technik, aby stanowić zagrożenie. Na przykład narzędzia programowe, które pozwalają użytkownikowi zlokalizować otwarte porty lub obejść ochronę hasłem, można łatwo wprowadzić do sieci. Cyberprzestępczość dotyka obecnie ponad 431 milionów dorosłych ofiar na całym świecie. Strategie dotyczące cyberprzestępczości powinny być ściśle zintegrowane ze strategiami cyberbezpieczeństwa, aby uwzględnić kluczowe elementy, takie jak podnoszenie świadomości, współpraca międzynarodowa i zdolność egzekwowania prawa. Cyberbezpieczeństwo zwykle odnosi się

do integralności naszej prywatności w Internecie, do bezpieczeństwa naszej infrastruktury krytycznej, do handlu elektronicznego, do zagrożeń militarnych i ochrony własności intelektualnej. Jest to ochrona systemów podłączonych do Internetu (np. sprzętu, oprogramowania i powiązanej infrastruktury), znajdujących się na nich danych oraz świadczonych przez nie usług przed nieautoryzowanym dostępem, uszkodzeniem lub niewłaściwym wykorzystaniem. Strategie cyberbezpieczeństwa, na przykład rozwój systemów ochrony technicznej lub edukacja użytkowników, aby nie stali się ofiarami cyberprzestępczości, mogą pomóc w zmniejszeniu ryzyka cyberprzestępczości. Poniższa tabela zawiera niektóre definicje cyberbezpieczeństwa

**Definicje cyberbezpieczeństwa**

Komitet ds. Systemów Bezpieczeństwa Narodowego: Zdolność do ochrony lub obrony użytkowania cyberprzestrzeni przez przedsiębiorstwo przed atakiem przeprowadzanym za pośrednictwem cyberprzestrzeni w celu: zakłócania, wyłączania, niszczenia lub złośliwego kontrolowania środowiska/infrastruktury obliczeniowej; lub niszcząc integralność danych lub kradzież kontrolowanych informacji.

Narodowy Instytut Standardów i Technologii: Proces ochrony informacji poprzez zapobieganie atakom, wykrywanie ich i reagowanie na nie. Podobnie jak ryzyko finansowe i reputacyjne, ryzyko cyberbezpieczeństwa wpływa na wyniki finansowe firmy. Może podnieść koszty i wpłynąć na przychody. Może zaszkodzić zdolności organizacji do innowacji oraz pozyskiwania i utrzymywania klientów

Międzynarodowa Organizacja Normalizacyjna: Zachowanie poufności, integralności i dostępności informacji w cyberprzestrzeni. Z kolei „Cyberprzestrzeń" definiowana jest jako „złożone środowisko powstałe w wyniku interakcji ludzi, oprogramowania i usług w Internecie za pomocą podłączonych do niego urządzeń technologicznych i sieci, które nie istnieje w żadnej fizycznej formie".

**NAJWAŻNIEJSZE CECHY NARODOWEGO PROGRAMU CYBERBEZPIECZEŃSTWA**

Na poziomie krajowym jest to wspólna odpowiedzialność wymagająca skoordynowanych działań związanych z zapobieganiem, przygotowaniem, reagowaniem i naprawą po incydentach ze strony organów rządowych, sektora prywatnego i obywateli, ponieważ cyberzagrożenie wpływa na całe społeczeństwo. Naród nie może odnieść sukcesu w zabezpieczaniu cyberprzestrzeni, jeśli działa w izolacji, zwłaszcza interesy sektora publicznego i prywatnego przeplatają się ze wspólną odpowiedzialnością za zapewnienie bezpiecznej i niezawodnej infrastruktury. Naród potrzebuje również strategii cyberbezpieczeństwa zaprojektowanej w celu kształtowania środowiska międzynarodowego i zbliżania narodów o podobnych poglądach w wielu kwestiach, takich jak standardy techniczne i dopuszczalne normy prawne dotyczące jurysdykcji terytorialnej, suwerennej odpowiedzialności i użycia siły. Normy międzynarodowe mają kluczowe znaczenie dla ustanowienia bezpiecznej i dobrze prosperującej infrastruktury cyfrowej. Cyberbezpieczeństwo nie jest już wyłącznie kwestią bezpieczeństwa komputerowego i jest uważane za kwestię polityki krajowej, ponieważ nielegalne korzystanie z cyberprzestrzeni może utrudnić działalność gospodarczą, zdrowie publiczne, bezpieczeństwo i bezpieczeństwo narodowe. Krajowy program bezpieczeństwa cybernetycznego powinien opracować plany, aby kraj był pewny siebie, zdolny i odporny w szybko zmieniającym się cyfrowym świecie. Poniżej przedstawiono, co ITU uważa za główne cechy holistycznego, wielostronnego i opartego na strategii programu cyberbezpieczeństwa. Kluczowe elementy, w tym interesariuszy cyberbezpieczeństwa, środki prawne, krajowy zespół reagowania na incydenty komputerowe oraz współpraca międzynarodowa, omówiono w kolejnych sekcjach.

**Elementy programu cyberbezpieczeństwa**

Odpowiedzialność za bezpieczeństwo cybernetyczne najwyższego szczebla: Najwyżsi przywódcy rządowi są odpowiedzialni za opracowanie strategii krajowej i wspieranie współpracy międzysektorowej na szczeblu lokalnym, krajowym i globalnym.

Krajowy Koordynator ds. Cyberbezpieczeństwa: Biuro lub osoba fizyczna nadzoruje działania w zakresie cyberbezpieczeństwa w całym kraju.

Krajowy punkt kontaktowy ds. cyberbezpieczeństwa: Organ złożony z wielu agencji służy jako punkt kontaktowy dla wszystkich działań związanych z ochroną cyberprzestrzeni danego kraju przed wszystkimi rodzajami cyberzagrożeń.

Środki prawne : zazwyczaj kraj dokonuje przeglądu i, jeśli to konieczne, opracowuje nowe przepisy prawa karnego, procedury i politykę w celu powstrzymania, reagowania i ścigania cyberprzestępczości.

Krajowe ramy cyberbezpieczeństwa : kraje zazwyczaj przyjmują ramy, które określają minimalne lub obowiązkowe wymagania dotyczące bezpieczeństwa w kwestiach takich jak zarządzanie ryzykiem i zgodność.

Zespół Reagowania na Incydenty Komputerowe (CIRT): Program oparty na strategii zawiera funkcje zarządzania incydentami z odpowiedzialnością krajową. Rola ta analizuje trendy cyberzagrożeń, koordynuje reagowanie i rozpowszechnia informacje wśród wszystkich zainteresowanych stron.

Świadomość i edukacja w zakresie bezpieczeństwa cybernetycznego: Powinien istnieć krajowy program mający na celu podnoszenie świadomości na temat zagrożeń cybernetycznych.

Partnerstwo w zakresie bezpieczeństwa cybernetycznego sektora publiczno-prywatnego: Rządy powinny tworzyć znaczące partnerstwo z sektorem prywatnym.

Program umiejętności i szkoleń w zakresie cyberbezpieczeństwa : program powinien pomóc w szkoleniu specjalistów ds. cyberbezpieczeństwa.

Współpraca międzynarodowa: Globalna współpraca jest niezbędna ze względu na transnarodowy charakter zagrożeń cybernetycznych

**INTERESARIUSZE W ZAKRESIE CYBERBEZPIECZEŃSTWA**

Zabezpieczenie krajowej cyberprzestrzeni będzie wymagało zbiorowego wysiłku. Każdy z nas, od rządu po jednostki, ma do odegrania ważną rolę.

**RZĄD**

Rządy mają obowiązek zapewnić, aby cyberprzestrzeń była wystarczająco odporna i godna zaufania, aby wspierać wzrost gospodarczy, wolności obywatelskie i ochronę prywatności oraz bezpieczeństwo narodowe. Chociaż kluczowe sektory naszej gospodarki znajdują się w rękach prywatnych, to rząd jest ostatecznie odpowiedzialny za zapewnienie ich narodowej odporności oraz, wraz ze swoimi partnerami w całej administracji, za utrzymanie podstawowych usług i funkcji w całym rządzie. Ponadto władze lokalne, stanowe i centralne przechowują ogromne ilości danych osobowych i rejestrów swoich obywateli, a także poufne informacje rządowe, co czyni je częstymi celami. W związku z tym władza wykonawcza rządu jest odpowiedzialna za ustalanie agendy zabezpieczenia wszystkich domen bezpieczeństwa narodowego, w tym cyberprzestrzeni. Według ITU, National Cybersecurity Strategy Guide, Zarząd pełni następujące role:

* Zdefiniowanie roli cyberprzestrzeni w osiąganiu krajowych celów rozwojowych

* Identyfikacja, analiza i łagodzenie zagrożeń dla realizacji interesów narodowych

* Sponsorowanie i pozyskiwanie krajowego programu cyberbezpieczeństwa

* Opracowanie przepisów dotyczących cyberprzestępczości, które mają zastosowanie na całym świecie i są interoperacyjne

* Zachęcanie do rozwoju bezpiecznych technologii, takich jak kryptografia

* Zarządzanie programami budowania zdolności ludzkich i instytucjonalnych

* Podpisanie międzynarodowych traktatów i konwencji dotyczących cyberbezpieczeństwa

* Formułowanie i obrona stanowisk w zakresie cyberbezpieczeństwa na forach regionalnych i globalnych

**WŁAŚCICIELE I OPERATORZY KRYTYCZNEJ INFRASTRUKTURY**

Podczas gdy rząd jest odpowiedzialny za ochronę i obronę kraju, sektor prywatny projektuje, buduje, posiada i obsługuje większość infrastruktur sieciowych, które wspierają zarówno użytkowników rządowych, jak i prywatnych. Przemysł i rządy ponoszą wspólną odpowiedzialność za bezpieczeństwo i niezawodność infrastruktury oraz dokonywane na niej transakcje. Powinny zatem ściśle współpracować, aby zająć się tymi współzależnościami, zwłaszcza w tych krajach, w których sprywatyzowane zostały krytyczne systemy infrastrukturalne w obszarach takich jak usługi komunalne, finanse i transport. W Stanach Zjednoczonych i Wielkiej Brytanii partnerstwo publiczno-prywatne było wielokrotnie określane jako „kamień węgielny" lub „centrum" strategii bezpieczeństwa cybernetycznego. Dlatego ważne jest, aby kluczowi właściciele infrastruktury i operacje wnosili wkład w opracowanie krajowej strategii ze względu na ich bezpośredni interes ekonomiczny w powodzeniu krajowego programu cyberbezpieczeństwa. Według ITU, National Cybersecurity Strategy Guide, właściciele i operatorzy infrastruktury krytycznej odgrywają następujące role w opracowywaniu strategii:

* Zapewnienie wglądu w to, jak dane cyberzagrożenia i luki w zabezpieczeniach wpływają na ich sektory

* Oferowanie informacji o tym, jak luki w zabezpieczeniach wpływają na zastrzeżone systemy i oprogramowanie

* Dzielenie się wiedzą o tym, co naprawdę działa, dzięki ich doświadczeniu w zakresie bezpieczeństwa operacyjnego

* Dzielenie się wiedzą na temat zasobów, sieci, systemów, obiektów i funkcji cybernetycznych

* Pokazanie, jak zrównoważyć cyberbezpieczeństwo z wydajnością i rentownością

* Przyczynianie się do wiedzy i doświadczenia w zakresie reagowania na incydenty

Parlament Europejski zatwierdził dyrektywę w sprawie bezpieczeństwa sieci i informacji, której celem jest poprawa współpracy i wymiany informacji na temat inicjatyw w zakresie cyberbezpieczeństwa między państwami członkowskimi, a także między sektorem publicznym i prywatnym. Dyrektywa wymaga, aby organizacje w niektórych sektorach infrastruktury krytycznej przyjęły praktyki zarządzania ryzykiem i zgłaszały poważne incydenty organom krajowym.

**BIZNES I ORGANIZACJE**

Firmy, organizacje sektora publicznego i prywatnego oraz inne instytucje przechowują dane osobowe, świadczą usługi i obsługują systemy w domenie cyfrowej. Łączność tych informacji zrewolucjonizowała

ich działalność. Jednak wraz z tą technologiczną transformacją pojawia się odpowiedzialność za ochronę posiadanych aktywów, utrzymanie świadczonych usług i włączenie odpowiedniego poziomu bezpieczeństwa do sprzedawanych produktów. Obywatele i konsumenci oraz ogół społeczeństwa oczekują od przedsiębiorstw i organizacji podjęcia wszelkich uzasadnionych kroków w celu ochrony ich danych osobowych i budowania odporności systemów i struktur, od których są zależne. Firmy i organizacje muszą również zrozumieć, że jeśli padną ofiarą cyberataku, ponoszą odpowiedzialność za konsekwencje.

**INDYWIDUALNI**

Cyberbezpieczeństwo jest niezbędnym czynnikiem dla osób i rodzin, a także firm, rządów i instytucji edukacyjnych. Podejmujemy praktyczne kroki, aby zabezpieczyć cenione przez nas aktywa w świecie fizycznym. W wirtualnym świecie powinniśmy zrobić to samo. Oznacza to spełnienie naszej osobistej odpowiedzialności za podjęcie wszelkich uzasadnionych kroków w celu ochrony nie tylko naszego sprzętu (np. naszych smartfonów i innych urządzeń), ale także danych, oprogramowania i systemów, które zapewniają nam wolność, elastyczność i wygodę w życiu prywatnym i zawodowym. Cisco sugeruje, aby w trybie online pamiętać o tym: „Stop. Myśleć. Łączyć". Zatrzymaj się na chwilę. Zastanów się, jak zadbamy o informacje i dane osobowe przed podjęciem działania. Oto niektóre działania, które każdy może wykonać:

* Nie otwieraj wiadomości ani załączników z nieznanych źródeł

* Używaj filtrów spamu, aby zapobiegać niechcianym i niebezpiecznym wiadomościom e-mail

* Aktualizuj swój komputer, zwłaszcza system operacyjny, przeglądarki internetowe i ochronę antywirusową/antyspyware

* Wybierz silne hasła, które nie są łatwe do odgadnięcia i unikaj adresu, imienia zwierzaka lub imienia dziecka

* Regularnie zmieniaj hasła

* Bądź mądry z tożsamością w serwisach społecznościowych

* Pamiętaj, aby przejrzeć i używać ustawień prywatności oraz zachować wszystkie oznaczone zdjęcia jako prywatne

* Nie udostępniaj informacji, które mogą pomóc ludziom ukraść naszą tożsamość osobistą

**ŚRODKI PRAWNE**

**RZĄDOWE WŁADZE PRAWNE**

Administracje krajowe są odpowiedzialne za cyberbezpieczeństwo, ponieważ cyberataki zagrażają interesom narodowym w sferze gospodarczej, dyplomatycznej i bezpieczeństwa narodowego. Według ITU, rządom krajowym często brakuje uprawnień prawnych do prowadzenia spójnego krajowego programu cyberbezpieczeństwa z następujących powodów:

• Sektor prywatny jest właścicielem większości krytycznej infrastruktury informatycznej.

• Cyberprzestrzeń zaciera granicę między normalnymi operacjami organów ścigania a operacjami wojskowymi.

• Globalna współpraca w zakresie cyberprzestępczości wymaga traktatów o ekstradycji i transgranicznych wyszukiwarkach internetowych, które mogą nie istnieć.

W związku z tym ITU zaleca, aby strategia środków prawnych zawierała strukturę zarządzania zapewniającą Zarządowi mandat prawny do mobilizacji wszystkich zasobów przed zagrożeniami cybernetycznymi. Chociaż lokalne warunki różnią się, mandat zazwyczaj:

* Zapewnia szefowi rządu uprawnienia prawne do tworzenia i finansowania krajowego programu cyberbezpieczeństwa

* Określa podstawę prawną utworzenia krajowego Zespołu Reagowania na Incydenty Komputerowe

* Daje uprawnienia do wyłączania krytycznego zasobu infrastruktury w przypadku zagrożenia cyberatakiem

* Stanowi podstawę do promowania umiejętności, szkoleń i świadomości w zakresie cyberbezpieczeństwa

* Definiuje podstawę prawną i operacyjną zintegrowanego i w pełni skoordynowanego partnerstwa sektora publiczno-prywatnego w zakresie cyberbezpieczeństwa

* Wspiera innowacje w cyberbezpieczeństwie, aby pomóc w opracowywaniu długoterminowych rozwiązań

* Przyznaje rządowi uprawnienia do udziału we współpracy międzynarodowej, dialogu i działaniach koordynacyjnych ukierunkowanych na cyberbezpieczeństwo, takich jak wzajemna pomoc

**RAMY ZARZĄDZANIA EGZEKWOWANIEM PRAWA**

Artykuł 1 Kodeksu postępowania dla funkcjonariuszy organów ścigania ONZ podkreśla, że rolą organów ścigania jest wypełnianie obowiązków nałożonych na nich przez prawo, „służąc społeczności i chroniąc wszystkie osoby przed czynami niezgodnymi z prawem". Skuteczne egzekwowanie prawa pomaga zapobiegać nielegalnemu korzystaniu z technologii informacyjno-komunikacyjnych, zniechęcać do niego, reagować na nie i wspierać jego ściganie. Dlatego strategia środków prawnych powinna uwzględniać stworzenie struktury zarządzania lub ram strategicznych w celu koordynowania działań organów ścigania, dochodzeń, polityki i regulacji przeciwko cyberprzestępczości. Według ITU, National Cybersecurity Strategy Guide, struktura zarządzania powinna:

* Określać role organizacji dochodzeniowych i organów ścigania

* Połączyć działania organów ścigania online i offline przeciwko wszelkim rodzajom przestępstw

* Zapewnić solidne i globalnie zharmonizowane podejście do działań organów ścigania

* Zapewnić organom ścigania niezbędne informacje i zasoby, aby zdobyć i utrzymać umiejętności skutecznego zwalczania cyberprzestępczości

* Stworzyć ramy dialogu i koordynacji organów ścigania na poziomie lokalnym, regionalnym i międzynarodowym

**GLOBALNA WALKA Z CYBERPRZESTĘPCZOŚCIĄ**

„Wymiar transgraniczny" przestępstwa cyberprzestępczości ma miejsce, gdy elementem lub istotnym skutkiem przestępstwa jest inne terytorium lub gdy część modus operandi przestępstwa znajduje się na innym terytorium. Według UNODC kraje, które odpowiedziały na kwestionariusz Comprehensive Study on Cybercrime, zgłosiły średnie regionalne od 30% do 70% cyberprzestępczości o wymiarze transnarodowym. Dlatego tak ważne jest, aby narody uczestniczyły w wysiłkach na rzecz opracowania i harmonizacji środków prawnych na całym świecie. Udział może być częścią przekrojowych wysiłków

w zakresie współpracy międzynarodowej. Kraje mogą również rozważyć włączenie środków prawnych do spójnej międzynarodowej strategii na rzecz cyberprzestrzeni. Na przykład brytyjska narodowa strategia cyberbezpieczeństwa określa następujące podejścia do ochrony długoterminowej przyszłości wolnej, otwartej, pokojowej i bezpiecznej cyberprzestrzeni, stymulując wzrost gospodarczy i wspierając bezpieczeństwo narodowe Wielkiej Brytanii.

**Narodowa Strategia Cyberbezpieczeństwa - Działania międzynarodowe**

• Wzmocnienie i zakorzenienie wspólnego rozumienia odpowiedzialnego zachowania państwa w cyberprzestrzeni;

• Opierać się na porozumieniu, że prawo międzynarodowe ma zastosowanie w cyberprzestrzeni;

• Kontynuować promowanie porozumienia w sprawie dobrowolnych, niewiążących norm odpowiedzialnego zachowania państwa;

• Wspierać rozwój i wdrażanie środków budowy zaufania;

• Zwiększenie naszej zdolności do zakłócania i ścigania cyberprzestępców przebywających za granicą, zwłaszcza w trudno dostępnych jurysdykcjach;

• Pomóż stworzyć środowisko, które pozwoli naszym organom ścigania współpracować w celu zapewnienia mniejszej liczby miejsc, w których cyberprzestępcy mogą działać bez obawy przed dochodzeniem i ściganiem;

• Promowanie odporności cyberprzestrzeni poprzez kształtowanie standardów technicznych regulujących na arenie międzynarodowej nowe technologie (w tym szyfrowanie), zwiększanie bezpieczeństwa cyberprzestrzeni w fazie projektowania oraz promowanie najlepszych praktyk;

• Pracować nad stworzeniem wspólnego podejścia wśród krajów o podobnych poglądach do takich możliwości, jak silne szyfrowanie, które mają konsekwencje transgraniczne;

• Budowanie zdolności innych do radzenia sobie z zagrożeniami dla Wielkiej Brytanii i naszymi interesami za granicą;

• W dalszym ciągu pomagać naszym partnerom w rozwijaniu ich własnego bezpieczeństwa cybernetycznego – ponieważ dzielimy jedną cyberprzestrzeń, wspólnie stajemy się silniejsi, gdy każdy kraj poprawia swoją własną obronę;

• Zapewnienie przygotowania NATO na konflikty XXI wieku, które rozegrają się zarówno w cyberprzestrzeni, jak i na polu bitwy;

• Współpracować z naszymi sojusznikami, aby umożliwić NATO działanie w cyberprzestrzeni równie skutecznie, jak na lądzie, w powietrzu i na morzu; oraz

• Zapewnienie, że „Londyński proces" globalnych konferencji na temat cyberprzestrzeni nadal promuje globalny konsensus w sprawie wolnej, otwartej, pokojowej i bezpiecznej cyberprzestrzeni.

**KRAJOWY ZESPÓŁ REAGOWANIA NA INCYDENTY KOMPUTEROWE**

Zespoły reagowania na incydenty komputerowe (CIRT) odgrywają ważną rolę w monitorowaniu, wykrywaniu, analizowaniu i badaniu cyberzagrożeń i incydentów cybernetycznych w odpowiedzi na rosnące zaawansowanie, częstotliwość i wagę cyberzagrożeń. Szybka i skuteczna reakcja na incydenty cybernetyczne może okazać się kluczowa dla zminimalizowania powstałych szkód i przyspieszenia

odzyskiwania. Według ITU, National Cybersecurity Strategy Guide, krajowy CIRT jest odpowiedzialny za:

* Zapewnienie wsparcia reagowania na incydenty wszystkim zainteresowanym stronom za pośrednictwem ustalonych, zaufanych, autoryzowanych i centralnie koordynowanych inicjatyw na poziomie krajowym;

* Rozpowszechnianie krytycznych informacji, takich jak wczesne ostrzeżenia i powiadomienia alarmowe, doradztwo w zakresie bezpieczeństwa oraz stosowanie najlepszych praktyk w zakresie bezpieczeństwa;

* Pełnienie funkcji pojedynczego punktu kontaktowego w zakresie zgłaszania i koordynacji incydentów cybernetycznych;

* Wykrywanie i identyfikacja anomalnej aktywności;

* Analizowanie zagrożeń cybernetycznych i rozpowszechnianie informacji ostrzegawczych o zagrożeniach cybernetycznych;

* Analizowanie i syntezowanie informacji o incydentach i lukach w zabezpieczeniach rozpowszechnianych przez innych, takich jak dostawcy, w celu zapewnienia oceny zainteresowanym stronom;

* Ustanowienie zaufanych mechanizmów komunikacyjnych i ułatwienie komunikacji między zainteresowanymi stronami w celu dzielenia się informacjami i rozwiązywania problemów związanych z cyberbezpieczeństwem;

* Opracowywanie strategii łagodzenia i reagowania oraz koordynowanie reakcji na incydenty;

* Udostępnianie danych i informacji o incydencie oraz odpowiednich odpowiedziach;

* Określanie trendów i długoterminowych strategii naprawczych;

* Publikowanie najlepszych praktyk w zakresie reagowania na incydenty i porad dotyczących zapobiegania;

* Koordynowanie współpracy międzynarodowej w zakresie incydentów cybernetycznych; oraz

* Budowanie potencjału we wszystkich powyższych obszarach przy użyciu zaawansowanych technologii i technik, ustalanie metod oraz badanie analiz i łagodzenia zagrożeń.

**WSPÓŁPRACA MIĘDZYNARODOWA**

Mobilność przestępców sprawia, że organy ścigania i organy sądowe muszą współpracować i pomagać państwu, które przejęło jurysdykcję. Ponieważ nie ma kompleksowych międzynarodowych ram prawnych ani ponadnarodowego organu, który byłby w stanie badać takie przestępstwa, przestępstwa międzynarodowe wymagają współpracy władz w zaangażowanych krajach. W celu zarządzania procesem wyrażania zgody na prowadzenie dochodzeń organów ścigania i wymiaru sprawiedliwości w sprawach karnych poza terytorium państwa istnieje szereg prawnych i nieformalnych porozumień między państwami, zarówno na poziomie dwustronnym, jak i wielostronnym. Oparte na Globalnej Agendzie Cyberbezpieczeństwa (GCA) ITU, holistyczne ramy koordynacji, rozwoju i wdrażania solidnej globalnej kultury cyberbezpieczeństwa zawierają następujące siedem celów strategicznych:

1) Opracowanie strategii rozwoju modelowego ustawodawstwa dotyczącego cyberprzestępczości, które ma zastosowanie na całym świecie i jest interoperacyjne z istniejącymi krajowymi i regionalnymi środkami legislacyjnymi;

2) Opracowanie globalnych strategii tworzenia odpowiednich krajowych i regionalnych struktur organizacyjnych oraz polityk dotyczących cyberprzestępczości;

3) Opracowanie strategii ustanowienia globalnie akceptowanych minimalnych kryteriów bezpieczeństwa i schematów akredytacji dla sprzętu i oprogramowania aplikacji i systemów;

4) Opracowanie strategii tworzenia globalnych ram obserwacji, ostrzegania i reagowania na incydenty w celu zapewnienia transgranicznej koordynacji pomiędzy nowymi i istniejącymi inicjatywami;

5) Opracowanie globalnych strategii tworzenia i zatwierdzania ogólnego i uniwersalnego systemu tożsamości cyfrowej oraz niezbędnych struktur organizacyjnych w celu zapewnienia uznawania cyfrowych danych uwierzytelniających ponad granicami geograficznymi;

6) Opracowanie globalnej strategii ułatwiającej budowanie potencjału ludzkiego i instytucjonalnego w celu zwiększenia wiedzy i know-how we wszystkich sektorach i we wszystkich wyżej wymienionych obszarach; oraz

7) Propozycje dotyczące ram globalnej wielostronnej strategii współpracy międzynarodowej, dialogu i koordynacji we wszystkich wyżej wymienionych obszarach.