NASK Cyber POLICY

NASK CERT.PL

secure Policy 2020

Strategia i regulacje w obszarze cyberbezpieczeństwa i nowoczesnych technologii

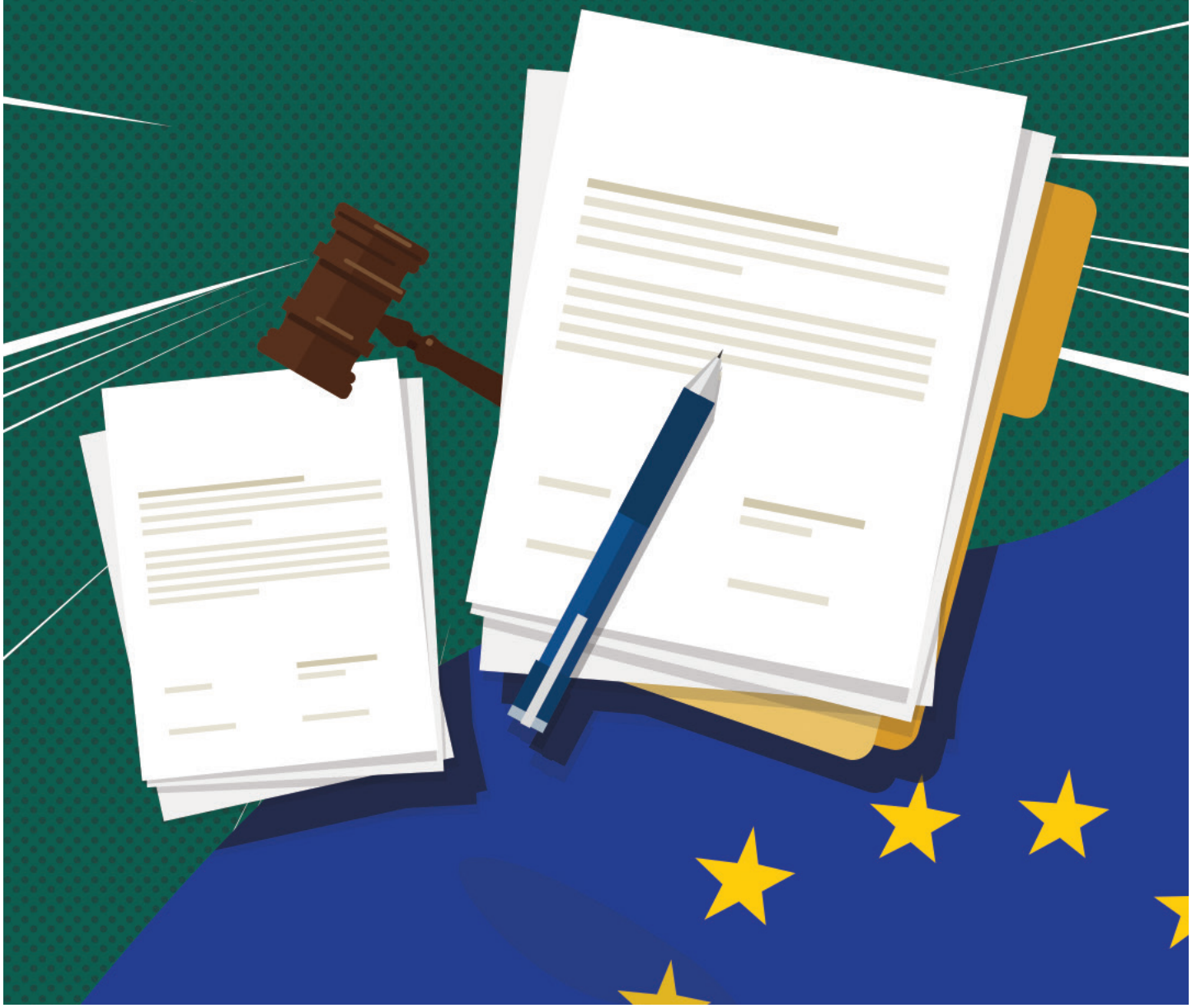
NASK Cyber POLICY

NASK CERT.PL

secure 2020

Część I

Regulacje krajowe i europejskie



Najnowsze inicjatywy KE w zakresie cyberbezpieczeństwa

Działania KE w zakresie cyberbezpieczeństwa są planowane na szczeblu politycznym i realizowane przy użyciu odpowiednich instrumentów i programów finansowych, takich jak: ***Łącząc Europę CEF, Cyfrowa Europa DEP, Horyzont 2020 i Horyzont Europa.***

Począwszy od 2013 roku, KE podjęła szereg inicjatyw zwiększających poziom cyberbezpieczeństwa państw członkowskich UE. Do najważniejszych działań w tym zakresie należy zaliczyć przyjęcie: Dyrektywy NIS, Aktu o Cyberbezpieczeństwie, propozycji rozporządzenia ustanawiającego Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa, zalecenia dotyczącego cyberbezpieczeństwa sieci 5G oraz skoordynowanego planu reagowania na incydenty i kryzysy cybernetyczne na dużą skalę („Blueprint").

Priorytetowe inicjatywy KE na rzecz zwiększenia poziomu cyberbezpieczeństwa UE w 2020 roku to przede wszystkim:

- **Zestaw narzędzi 5G**

  KE stoi na stanowisku, że wyłącznie wspólne działania na poziomie poszczególnych państw członkowskich UE oraz unijnej administracji zapewnią odpowiedni poziom bezpieczeństwa sieci 5G w UE. Proces ten jest wieloetapowy i wymaga ścisłej współpracy pomiędzy wieloma grupami roboczymi (odpowiedzialnymi za wyznaczenie celów strategicznych), podgrupą ds. standaryzacji i cyfryzacji, BEREC oraz KE. Zestaw narzędzi 5G powstał w oparciu o zaprezentowaną w 2019 roku unijną skoordynowaną ocenę ryzyka związanego z cyberbezpieczeństwem sieci 5G. KE zapowiedziała, że do końca 2020 roku zostanie zakończony przegląd technicznych i strategicznych zaleceń, które mają skutecznie ograniczyć ryzyko sieci 5G w UE.

  Czytaj więcej:

  https://cyberpolicy.nask.pl/zestaw-narzedzi-toolbox-dla-bezpieczenstwa-sieci-5g/ oraz https://cyberpolicy.nask.pl/analiza-5g-toolbox-implementation-report/

- **Rewizja Dyrektywy NIS**

  Głównymi przedmiotami analizy związanej z rewizją Dyrektywy NIS są: identyfikacja operatorów usług kluczowych, rola dostawców usług cyfrowych, zakres dyrektywy NIS, wymogi w zakresie cyberbezpieczeństwa, proces zgłaszania incydentów, rola władz krajowych oraz zespołów CSIRT, współpraca na poziomie unijnym. Zakończenie procesu rewizji Dyrektywy NIS zostało zaplanowane na koniec 2020 roku. W ramach dotychczasowych działań przeglądowych KE zidentyfikowała następujące problemy związane ze wdrażaniem Dyrektyw NIS:

  - Duże różnice w implementacji dyrektywy i identyfikacji operatorów usług kluczowych (OUK). Ponieważ Dyrektywa jest harmonizacją minimalną, każde państwo członkowskie ma dużą dowolność w implementacji jej zapisów. W efekcie mamy różne progi identyfikacji operatorów usług kluczowych oraz różne progi raportowania incydentów teleinformatycznych. Skutkuje to dużą fragmentyzacją rynku, a operatorzy świadczący usługi w kilku państwach członkowskich muszą się stosować do odmiennych reżimów prawnych.
  - Niewystarczający zakres Dyrektywy. Niektóre sektory i operatorzy, pomimo kluczowej działalności i istotności z punktu widzenia zapewnienia cyberbezpieczeństwa, nie znalazły się w zakresie Dyrektywy. Efektem jest niewystarczająca wiedza CSIRT na temat poziomu cyberbezpieczeństwa w krajach członkowskich i brak koordynacji na poziomie UE w tym zakresie.

  KE zwraca uwagę na konieczność dostosowania obowiązującego prawa do szybkich zmian i nowych zagrożeń. Zakres obecnej Dyrektywy odpowiada sytuacji w latach 2013 – 2016 i nie adresuje najnowszych wyzwań, związanych z rozwojem technologii takich jak: bezpieczeństwo łańcucha dostaw, czy kwestia dostawców usług cyfrowych – coraz większe wykorzystanie usług chmurowych w wielu dziedzinach gospodarki.

  KE rozważa cztery scenariusze zmian w Dyrektywie NIS. Pierwsze dwa to miękkie mechanizmy:

  - Podejście ewolucyjne – oznacza wykorzystanie obecnych zapisów i pełne ich wdrożenie.
  - Przygotowanie wytycznych, które doprecyzują obecnie obowiązujące zapisy prawne i wprowadzą większą harmonizację przepisów na poziomie UE (np. w zakresie identyfikacji operatorów i progów raportowania dla incydentów).

  Dwa kolejne scenariusze zmian w Dyrektywie NIS dotyczą treści przepisów:

  - Doprecyzowanie zapisów samej Dyrektywy, w tych miejscach, gdzie istnieje taka konieczność (zmiana treści Dyrektywy).
  - Przyjęcie nowego aktu, który zastąpi Dyrektywę i wprowadzi większą harmonizację (być może w formie rozporządzenia).

- **Wspólna Jednostka ds. Cyberbezpieczeństwa**

  KE w nowej strategii ***Kształtowanie cyfrowej przyszłości Europy*** przedstawiła plan utworzenia wspólnej jednostki ds. Cyberbezpieczeństwa (***Joint Cyber Unit***). Głównym zadaniem jednostki będzie koordynacja współpracy operacyjnej, a także budowanie zaufania i dostarczanie kluczowych usług państwom członkowskim UE. Zdaniem KE taka inicjatywa pozwoli lepiej chronić europejską infrastrukturę, wzmocnić jednolity rynek cyberbezpieczeństwa, a także jednocześnie budować sojusze z partnerami światowymi promując przy tym europejski model cyfryzacji.

  Czytaj więcej:

  https://cyberpolicy.nask.pl/ksztaltowanie-przyszlosci-cyfrowej-europy-nowa-cyfrowa-strategia-ue/

Prezentację na temat inicjatyw KE w obszarze cyberbezpieczeństwa wygłosił Jakub Boratyński, przedstawiciel Komisji Europejskiej w Polsce.

NASK Cyber POLICY · NASK CERT.PL · secure 2020

Inicjatywy KE w 2020 roku w obszarze cyberbezpieczeństwa

Zestaw narzędzi 5G

- Zestaw technicznych i strategicznych zaleceń dotyczących bezpieczeństwa sieci 5G
- Zestaw narzędzi 5G powstał w oparciu o unijną skoordynowaną ocenę ryzyka związanego z cyberbezpieczeństwem sieci 5G
- Promowanie współpracy na poziomie państw członkowskich i unijnej administracji

Rewizja Dyrektywy NIS

Zidentyfikowane problemy związane z wdrażaniem Dyrektywy NIS

- Różnice w implementacji Dyrektywy i identyfikacji operatorów usług kluczowych
- Niewystarczający zakres dyrektywy

Zakończenie procesu rewizji pod koniec 2020 roku

Obszary problemowe

- Identyfikacja operatorów usług kluczowych
- Rola dostawców usług cyfrowych
- Zakres dyrektywy NIS
- Wymogi w zakresie cyberbezpieczeństwa
- Proces zgłaszania incydentów
- Rola władz krajowych i zespołów CSIRT

Wspólna jednostka ds. cyberbezpieczeństwa

- Plan utworzenia został zaprezentowany w strategii „Kształtowanie cyfrowej przyszłości Europy”
- Główne zadania: koordynacja współpracy operacyjnej, budowanie zaufania i dostarczanie kluczowych usług państwom członkowskim UE
- Jednostka pozwala lepiej chronić europejską infrastrukturę, wzmocni jednolity rynek cyberbezpieczeństwa, i także budować sojusze z partnerami światowymi

Działania Ministerstwa Cyfryzacji związane z wdrażaniem Ustawy o Krajowym systemie cyberbezpieczeństwa i propozycje zmian w ustawie

Ustawa o Krajowym Systemie Cyberbezpieczeństwa (UoKSC) weszła w życie 28 sierpnia 2018 roku. W tym roku minęły dokładnie 2 lata od jej wdrożenia.

Krajowy System Cyberbezpieczeństwa – 2 lata po wdrożeniu UoKSC:

- Wyznaczono 162 operatorów usług kluczowych[1], a także zidentyfikowano ok. 40 dostawców usług cyfrowych[2].
- Rośnie liczba zgłaszanych incydentów. W 2019 roku zarejestrowano 9 incydentów poważnych. Do 30.09.2020 roku było to już 27 incydentów, większość w sektorze bankowym.
- Zgłaszane incydenty najczęściej dotyczą złośliwego oprogramowania, obraźliwych i nielegalnych treści oraz spamu.
- Obserwujemy nasilenie ataków typu ransomware, które polegają na zaszyfrowaniu danych w celu wymuszenia okupu.

Wśród zidentyfikowanych problemów znalazły się:

- Kwestia incydentów w podmiotach publicznych. Z doświadczeń wynika, że samorządy nie zgłaszają incydentów w podmiotach publicznych (lub też zgłaszają je z opóźnieniem). Często też decydują się na zapłatę okupu lub wynajęcie zewnętrznych firm, które oferują usługę odzyskania straconych danych.
- Ograniczony rozwój sektorowych i branżowych zespołów cyberbezpieczeństwa. Na dzień 1.10.2020 powstał tylko jeden taki zespół – CSIRT KNF, a także jedno centrum wymiany informacji ISAC – sektor kolejowy.
- Wykorzystywanie przestarzałych technologicznie rozwiązań, niedobór wyspecjalizowanych kadr i finansowania, brak właściwych struktur u operatorów usług kluczowych – to wszystko prowadzi do trudności w skutecznym reagowaniu na incydenty.

We wrześniu 2020 Ministerstwo Cyfryzacji rozpoczęło publiczne konsultacje nowelizacji UoKSC. Projekt uwzględnia uwagi zgłaszane przez podmioty w trakcie dotychczasowych 2 lat funkcjonowania ustawy. Wśród najważniejszych propozycji zmian znalazły się:

- Rozszerzenie listy podmiotów KSC o przedsiębiorstwa komunikacji elektronicznej i utworzenie CSIRT Telco na poziomie CSIRTów sektorowych.
- Wprowadzenie do KSC operacyjnych centrów bezpieczeństwa SOC i centrów wymiany i analiz informacji ISAC.
- Możliwość prowadzenia oceny ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów KSC.
- Nowe instrumenty dla Pełnomocnika Rządu ds. Cyberbezpieczeństwa, które mają przyczynić się do skutecznej reakcji państwa w przypadku incydentu krytycznego.
- Kary za nieprzestrzeganie obowiązków UoKSC dostosowane do wysokości obrotu operatorów.

Prezentację na temat zmian w Ustawie o Krajowym Systemie Cyberbezpieczeństwa wygłosił Robert Kośla, Dyrektor Departamentu Cyberbezpieczeństwa Ministerstwo Cyfryzacji.

1 Stan na dzień 1.10.2020 r.
2 Stan na 30.06.2020 r.

NASK Cyber POLICY · NASK CERT.PL · secure 2020

2 lata funkcjonowania

Krajowego Systemu Cyberbezpieczeństwa w Polsce:

Stan na koniec 2020 r.

- Incydenty: złośliwe oprogramowanie, nielegalne treści i spam
- Coraz więcej zgłaszanych incydentów
- Nasilenie ataków ransomware
- 162 operatorów usług kluczowych i 40 dostawców usług

Zidentyfikowane problemy

- Niedojrzałość systemu (przestarzałe rozwiązania, niedobór kadry, brak struktur)
- Brak zgłaszania incydentów w podmiotach publicznych
- Ograniczony rozwój sektorowych zespołów cyberbezpieczeństwa

Nowelizacja UoKSC

- Wprowadzenie do KSC SOC i ISAC
- Włączenie do KSC przedsiębiorstw komunikacji elektronicznej
- Ocena ryzyka dostawcy sprzętu i oprogramowania podmiotów KSC
- Kary dostosowane do wysokości obrotu operatorów
- Utworzenie CSIRT Telco

Debata: Krajowy System Cyberbezpieczeństwa – co działa, a co nie? Co wynika dla Polski z europejskich regulacji i dokumentów strategicznych

W związku z dwuletnim funkcjonowaniem UoKSC, a także trwającą w tym roku nowelizacją ustawy oraz rewizją Dyrektywy NIS, coraz częściej pojawiają się pytania o wady i zalety krajowego systemu cyberbezpieczeństwa. Ustawa to pierwsze w Polsce prawo regulujące kwestie cyberbezpieczeństwa w sposób horyzontalny. Niewątpliwą zaletą UoKSC jest szerszy, niż w dyrektywie NIS, zakres podmiotowy, a także włączenie w system administracji państwowej i sektora telekomunikacji (pośrednio). Wciąż brakuje jednak kanałów bezpośredniej wymiany informacji. Nie jasna jest także kwestia dostawców usług cyfrowych, którzy zostali objęci lżejszą regulacją (tzw. ***light touch approach***), przez co trudno ich zidentyfikować i skłonić do raportowania incydentów.

Aktualnie największe wyzwania dla Krajowego Systemu Cyberbezpieczeństwa, związane również z rekonstrukcją rządu to:

- Konieczność reorganizacji związana z likwidacją MC i przeniesieniem działu informatyzacji pod Kancelarię Prezesa Rady Ministrów. Zmiana ta jest również szansą na większą decyzyjność w kwestiach informatyzacji – bezpośredni nadzór premiera nad działem.
- Ograniczone środki finansowe i konieczność realizacji zadań z wykorzystaniem minimalnego finansowania w przyszłym roku.
- Realizacja Strategii Cyberbezpieczeństwa RP 2019 – 2024 (link: https://cyberpolicy.nask.pl/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024/). Strategia wyznaczyła kierunki – powstał plan działań, który teraz należy zatwierdzić i zacząć realizować. W skali państwa brak jednak finansowania na te działania.

UoKSC umożliwia powołanie sektorowego zespołu ds. cyberbezpieczeństwa, którego rolę może pełnić również sektorowy ISAC – centrum wymiany i analiz informacji, mniej sformalizowana, oddolna inicjatywa. W tym roku w Polsce utworzono: Sektorowy Zespół ds. Cyberbezpieczeństwa Urzędu Komisji Nadzoru Finansowego (CSIRT KNF) i ISAC – Kolej w podsektorze transportu. CSIRT KNF został powołany przez UKNF, a więc organ właściwy ds. cyberbezpieczeństwa w sektorze finansów i infrastruktury rynków finansowych. ISAC – Kolej jest natomiast formą samoorganizacji sektora, wspieraną przez ministra właściwego ds. transportu i CSIRT NASK.

Największe wyzwania w tworzeniu sektorowych CSIRT/ISAC:

ISAC	CSIRT sektorowy
Podmioty wchodzące w skład ISAC to w pewien sposób konkurencja rynkowa, dlatego widoczny jest brak zaufania i niechęć do dzielenia się poufnymi informacjami. Najtrudniej jest przekonać członków ISAC, że wspólne bezpieczeństwo sektora służy wszystkim, a konkurencja nie powinna obejmować kwestii cyberbezpieczeństwa.	Brak zasobów kadrowych wynikający z niewielu specjalistów na rynku i bardzo wysokich wynagrodzeń. To jest wyzwanie dla wszystkich Organów Właściwych.
Zrozumienie, że skoro cyberprzestępcy działają w sojuszach, to również obrona powinna takie sojusze zawierać dla dobra całego sektora.	Konieczność budowania zaufania podmiotów do CSIRT KNF, który znajduje się w instytucji nadzorującej. Podmioty obawiają się, że zgłoszone przez nich incydenty będą powodem kontroli przez instytucję nadzorującą, choć funkcje te zostały w organizacji rozdzielone.
Brak usankcjonowania w ustawie.	Konieczność zbudowania relacji z podmiotami w formie roboczych konsultacji opartych na zaufaniu, a nie relacji: instytucja podległa ws. instytucja nadzorowana.

W projekcie nowelizacji UoKSC przewidziano obowiązkowe dla wszystkich Organów Właściwych ds. cyberbezpieczeństwa powołanie CSIRT sektorowych oraz usankcjonowanie ISAC poprzez utworzenie ich rejestru, prowadzonego przez ministra właściwego ds. informatyzacji.

Na uwagę zasługuje fakt, że ponieważ CSIRT sektorowe obejmą przede wszystkim podmioty wyznaczone przez Organy Właściwe jako operatorzy usług kluczowych, samoorganizacja sektora w ISAC, może być komplementarna do tych działań i wzmacniać bezpieczeństwo całego sektora.

W związku z nowelizacją UoKSC oraz rewizją dyrektywy NIS, która wpłynie na kształt regulacji z zakresu cyberbezpieczeństwa w państwach członkowskich, nieuniknione są zmiany w Krajowym Systemie Cyberbezpieczeństwa. Uczestnicy panelu, za najważniejsze wyzwania w perspektywie dwóch najbliższych lat uznali:

- Uruchomienie systemu S46[3] w pełnej skali.
- Wzrost świadomości z zakresu cyberbezpieczeństwa nie tylko wśród podmiotów UoKSC, ale również w całym społeczeństwie.
- Powstanie CSIRT sektorowych we wszystkich sektorach kluczowych.
- Realna troska o cyberbezpieczeństwo, a nie jedynie realizacja obowiązków ustawowych.

W debacie na temat: „Krajowy System Cyberbezpieczeństwa – co działa a co nie?" wzięli udział: Krzysztof Silicki (NASK), Krzysztof Zieliński (Urząd Komisji Nadzoru Finansowego), Dariusz Binkowski (Ministerstwo Klimatu), Grzegorz Kuta (PKP Polskie Linie Kolejowe S.A), Robert Kośla (Ministerstwo Cyfryzacji). Debatę prowadziła dr Magdalena Wrzosek (NASK).

3 Zgodnie z art. 46 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2018 r., poz. 1560t.j. Dz. U. z 2020 r. poz. 1369) minister właściwy do spraw informatyzacji zapewnia rozwój lub utrzymanie systemu teleinformatycznego wspierającego:
1) współpracę podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa;
2) generowanie i przekazywanie rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa;
3) zgłaszanie i obsługę incydentów;
4) szacowanie ryzyka na poziomie krajowym;
5) ostrzeganie o zagrożeniach cyberbezpieczeństwa.
(https://www.nask.pl/pl/projekty-dofinansowane/projekty-realizowane-ze/3957,Rozwoj-systemu-teleinformatycznego-S46.html)

NASK Cyber POLICY NASK CERT.PL secure 2020

Aktualne wyzwania dla KSC

Realizacja Strategii Cyberbezpieczeństwa RP 2019-2024 - wdrożenie planu działania

Likwidacja MC i przeniesienie działu informatyzacja pod KPRM

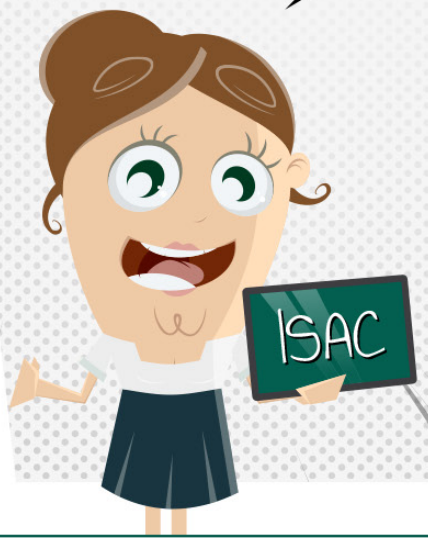
Ograniczone środki finansowe

ISAC/CSIRT sektorowy

Przekonanie uczestników, że wspólne bezpieczeństwo sektora służy wszystkim

Brak usankcjonowania w ustawie

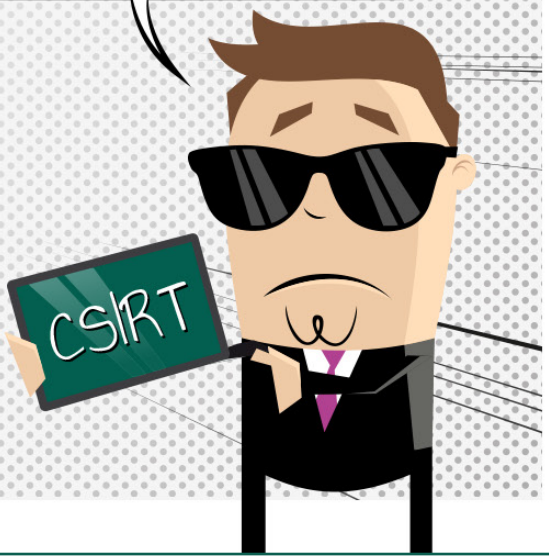
Namówienie do współpracy podmiotów, które na rynku są konkurencją



Brak zasobów kadrowych, niedobór specjalistów na rynku

Konieczność zbudowania zaufania pomiędzy CSIRT a podmiotami

Przejście z relacji nadzorującej na opartą na zaufaniu



NASK Cyber POLICY

NASK CERT.PL

secure 2020

Część II

Rewolucja cyfrowa w czasach pandemii

Transformacja cyfrowa w dobie COVID 19

W czasie pandemii COVID-19 pracodawcy inwestują w nowe technologie, które nie tylko pomagają zarządzać obecnym kryzysem, ale także pozwalają przygotować przedsiębiorstwa na przyszłe zagrożenia. Warto podkreślić, że transformacja cyfrowa, którą obserwujemy niemal w każdym obszarze działalności człowieka nie ogranicza się wyłącznie do technologii – to proces szerokich zmian społeczno-gospodarczych, które następują wraz z rozwojem technologii. Zmiany te mają wpływ na globalną gospodarkę i są obserwowane na rynku pracy, w przedsiębiorstwach i organizacjach oraz w środowisku konsumentów.

Fundamentalne znaczenie dla cyfrowej rewolucji mają technologie intensyfikujące, czyli technologie, które jednocześnie korzystają i rozszerzają możliwości współczesnych komputerów. Do technologii intensyfikujących należą:

- Rozwiązania chmurowe
- Internet Rzeczy
- Sztuczna Inteligencja
- Robotyzacja
- Blockchain

Najważniejsze zmiany obserwowane w czasie pandemii COVID-19 w obszarze technologii cyfrowych

- Roboty bezkontaktowe znalazły szerokie zastosowanie w czasie pandemii COVID-19 – głównie w szpitalach, ale także w centrach handlowych, na lotniskach czy dworcach. Mimo, że urządzenia tego typu były wykorzystywane już od dawna, to obecna sytuacja wymusiła na producentach zmianę ich przeznaczenia i przeprogramowanie. Obecnie bezkontaktowe roboty m.in. przekazują pacjentom informacje, dostarczają leki, dezynfekują dłonie lub duże powierzchnie.
- W czasie pandemii COVID-19 internetowe platformy sprzedażowe notują zwiększony ruch, a firmy deklarują istotny wzrost wykorzystania internetowych kanałów sprzedaży i obsługi klientów. Zdaniem analityków trend ten ma utrzymać się również po ustąpieniu pandemii. Zarówno platformy sprzedażowe, jak i konsumenci doceniają wygodę, prostotę i potencjał sprzedaży internetowej.
- Jak pokazują wyniki badań przeprowadzonych przez Salesforce, aż 74% konsumentów oczekuje, że firmy zaczną wykorzystywać istniejące technologie w nowy sposób. Taka postawa konsumentów wywiera presję na producentach technologii, pobudza ich innowacyjnosc i konkurencję.
- Transformacja cyfrowa zmienia rynek pracy. Do aktywności wykonywanych wyłącznie przez ludzi będą należały takie czynności jak: zarządzanie ludźmi, nierutynowe zadania fizyczne, nierutynowe zadania kognitywne, współpraca z ludźmi i przedsiębiorczość. Do aktywności hybrydowych, czyli zadań wykonywanych przez człowieka i maszynę będzie należało: szukanie niestandardowych rozwiązań, rozwiązywanie złożonych problemów, krytyczne myślenie. Do aktywności wykonywanych wyłącznie przez maszyny będzie należało: wykonywanie zadań rutynowych, autonomiczne podejmowanie decyzji, zbieranie i analiza danych, przestrzeganie procedur i standardów.
- Jak wynika z raportu DESI 2019 polski rynek pracy nie jest obecnie przygotowany na zmiany spowodowane przez cyfrową rewolucję. Jedynie co piąty Polak posiada ponadpodstawowe kompetencje cyfrowe, co plasuje Polskę na 24 miejscu w UE. Warto podkreślić, że polscy pracodawcy niechętnie zapewniają szkolenia podnoszące kompetencje cyfrowe swoich pracowników.
- Zdaniem ekspertów pandemia COVID-19 może przyczynić się do upowszechnienia na stałe modelu hybrydowego i częściowej pracy zdalnej.

Prezentację na temat transformacji cyfrowej w czasie pandemii COVID-19 wygłosiła Satia Rożynek z DELAB UW.

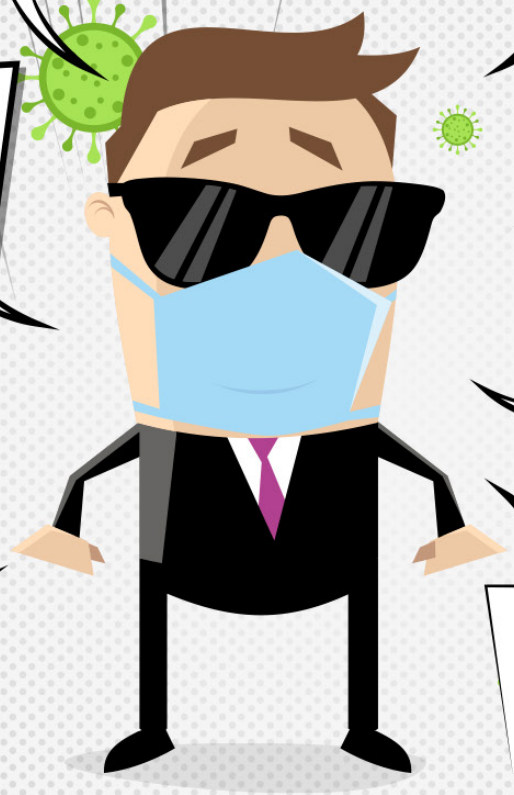
NASK Cyber POLICY NASK CERT.PL secure 2020

Zwiększone inwestycje pracodawców w nowe technologie

Wzrost znaczenia technologii intensyfikujących

- Rozwiązania chmurowe
- Internet Rzeczy
- Sztuczna Inteligencja
- Robotyzacja
- Blockchain

Istotny wzrost sprzedaży detalicznej za pośrednictwem internetowych kanałów sprzedaży



Wzrost innowacyjności i konkurencji wśród producentów nowych technologii

Dynamiczne zmiany na rynku pracy, w przedsiębiorstwach, organizacjach oraz w środowisku konsumentów

Konieczność przeprogramowania urządzeń, które były wykorzystywane przed wybuchem pandemii (np. bezkontaktowe roboty)

Transformacja cyfrowa w czasie pandemii COVID-19

Transformacja cyfrowa w czasach pandemii – przywództwo i odpowiedzialność liderów

Pandemia znacznie wpłynęła na świat biznesu. Ponieważ obecnie trudno o obszaru biznesu, gdzie nowe technologie nie miałyby znaczenia, w wielu przedsiębiorstwach i organizacjach czas pandemii przyczynił się do wdrożenia strategii cyfrowych. Firmy, które potrafiły szybko dostosować się do zmiany i wprowadzić innowacje odniosły sukces.

Udana transformacja cyfrowa zależy w dużej mierze od tego jak firma zarządza cyfrową transformacją, a nie tylko od tego czy wdraża same nowe technologie. Transformacja cyfrowa oprócz wdrażania zmian opartych o wykorzystanie nowoczesnych technologii w przedsiębiorstwach, polega również na zmianie stylu myślenia oraz na tworzeniu nowych możliwości rozwojowych. Jest wiec to zmiana nie tylko czysto technologiczna, ale również kulturowa.

W czasie pandemii, transformacja cyfrowa stała się nie tylko odpowiedzialnością kilku doświadczonych liderów w dziedzinie technologii, ale obowiązkiem każdego lidera w organizacji.

Kryzys jest iloczynem takich składników jak:

Z – zmiana, gotowość do zmian,

N – poziom niezadowolenia z istniejącego stanu,

W – wizja, jasno określony i dostatecznie atrakcyjny stan pożądany (cel, przewidywane efekty),

P – poparcie niektórych autorytetów,

S – pierwsze małe sukcesy, pierwsze praktyczne działania w kierunku stanu pożądanego,

K – koszty zmiany (w postaci energii, emocji, wysiłku, nakładów finansowych).

Kryzys jako pretekst do zmian

$$Z = f\{(N \times W \times P \times S) > K\}$$

Żeby doszło do zmian wypadkowa tych składników musi być większa niż koszty zmian, czyli włożona energia, emocje, wysiłek, czy też nakłady finansowe.

Pandemia najbardziej wpłynęła na czynnik jakim jest poziom niezadowolenia z istniejącego stanu. Wiele firm w czasie pandemii znalazło się w jak trudnej znalazło się sytuacji – zmniejszyły się przychody, pojawiły się trudności w operacyjnym działaniu, rynek stał się niepewny. To wszystko wpłynęło na niepewność pracowników i ich niezadowolenie wywołane w tym przypadku nie samą zmianą, a brakiem wprowadzenia zmian. Zaistniała zatem szansa wprowadzenia zmian, która dzięki odpowiedniej wizji, czyli jasnego i dostatecznie atrakcyjnego stanu, przedstawionej przez liderów, mogła okazać się sukcesem.

Najlepsze rezultaty osiągają Ci liderzy, którzy wprowadzają drobne konkretne działania, które przynoszą szybkie sukcesy oraz są empatyczni – rozumieją obawy swoich pracowników oraz partnerów w otoczeniu, solidaryzują się z ich pragnieniami, zapewniają wsparcie. Dzięki temu budują zaangażowanie swoich pracowników.

Wizja jutra

- Już dziś liderzy powinny myśleć o czasach postpandemicznych.
- Każdy lider powinien zaakceptować ryzyko, jakie niesie ze sobą wdrażanie nowych technologii.
- Zainicjonowane dziś, wdrożone i zweryfikowane pozytywnie cyfrowe zmiany, staną się nową normalnością.
- Dzięki temu drzwi, którymi weszliśmy do tego kryzysu nie będą drzwiami, którymi z niego wyjdziemy.

Potrzebna jest także umiejętność rozumienia, jak nowe technologie wpływają na współczesny świat. Dzięki zaangażowaniu liderów możemy wyjść z kryzysu wzmocnieni:

- z bardziej zaangażowanymi pracownikami,
- wdrożonymi nowymi cyfrowymi technologiami,
- większą społeczną wrażliwością na otoczenie,
- oraz zaufaniem do przyszłego kierunku rozwoju organizacji.

Prezentację na temat transformacji cyfrowej w czasie pandemii COVID-19 wygłosił dr hab. Rafał Mrówka, prof. SGH w Katedrze Teorii Zarządzania.

NASK Cyber POLICY

NASK CERT.PL

secure 2020

Transformacja cyfrowa w czasach pandemii

Transformacja cyfrowa to wdrażanie technologii, ale także zmiana myślenia oraz tworzenie nowych możliwości

Kryzys jako pretekst do pozytywnych zmian

- Pandemia jest sojusznikiem wprowadzenia zmian – to czas wdrażania strategii cyfrowych
- Dzięki zaangażowaniu liderów możemy wejść z kryzysu wzmocnieni

Wizja jutra

- Każdy lider powinien zaakceptować ryzyko jakie niesie ze sobą wdrażanie nowych technologii
- Już dziś liderzy powinny myśleć o czasach postpandemicznych
- Zainicjonowane dziś, wdrożone i zweryfikowane pozytywnie cyfrowe zmiany staną się nową normalnością

Transformacja cyfrowa jest teraz obowiązkiem każdego lidera

Debata oksfordzka: Czy COVID 19 wpłynął na przebieg cyfrowej rewolucji?

Od początku wybuchu pandemii, trwają dyskusje i spekulacje na temat tego w taki sposób wpłynęła ona na przebieg cyfrowej rewolucji – czy była pewnego rodzaju katalizatorem, który tylko przyspieszył nieuniknione zmiany, czy też wprowadziła zupełnie nową jakość i całkowicie zmieniła jej przebieg.

Pandemia nie wpłynęła na przebieg cyfrowej rewolucji, a tylko przyspieszyła procesy które i tak były nieuniknione.	**Pandemia wpłynęła na przebieg cyfrowej rewolucji i znacznie ją zmieniła.**
Rozwój technologii to nie tylko sama technologia, ale także otoczenie społeczno – ekonomiczne. Pandemia przyspieszyła i wymusiła wykorzystanie technologii, ale warto zwrócić uwagę, że w wielu państwach np. w Skandynawii te procesy już działały. Od dłuższego czasu mówiło się także o pracy zdalnej, jednak w wielu firmach kierownictwo było oporne. Pandemia sprawiła, że nie było wyjścia.	Rewolucja cyfrowa to przede wszystkim zmiana mentalna i w tym zakresie pandemia zmieniła bardzo dużo. Masowa praca zdalna spowodowała znaczną zmianę z sposobie myślenia i wykonywania codziennych obowiązków. Mamy realane wykorzystywanie technologii.
Choć narracja związana z COVID-19 była wykorzystywana w incydentach cyberbezpieczeństwa w czasie pandemii, to jednak charakter incydentów nie uległ zmianie.	Pandemia sprawiła, że w wielu firmach pojawiło się zrozumienie tego, jak ważnym elementem jest cyberbezpieczeństwo i wzrosła świadomość wyzwań z nim związanych wśród kadry zarządczej.
W czasie pandemii nie powstała żadna nowa technologia. Technologie, które są wykorzystywane już istniały. To co uległo zmianie to ich masowość i powszechność.	Pandemia zmusiła ludzi do realnego wykrzywiania technologii. Jest to trwała zmiana, której nie da się już odwrócić. Wyraźnie też było widać, że ludzie nie korzystają z każdej technologii, ale tylko z tej, która jest przydatna. Pandemia spowodowała także wzorst inwestycji w technologię.
Choć pandemia spowodowała przeniesienia się wielu obszarów życia społecznego do sieci, to jednak ludzie pozostają ludźmi i ich zachowania nie zmieniły się. Z konieczności korzystają z technologii, ale jest to jedynie narzędzie do utrzymania codziennego życia w “nowej normalności”, a nie głębsza przemiana wzorców zachowań.	Pandemia nie wpłynęła na wykorzystanie technologii przez firmy, ale przez zwykłych obywateli, którzy nagle otworzyli głowy na szybką, cyfrową przemianę. Zrozumieli, że zmiana jest możliwa.
	Do tej pory transformacja cyfrowa była bardziej modą/trendem, o której jedynie się rozmawiało. Nagle stała się realna i zmusiła firmy do konkretnych działań np. przeniesienia sprzedaży i działalności do sieci.

NASK Cyber POLICY NASK CERT.PL secure 2020

Pandemia nie wpłynęła na przebieg cyfrowej rewolucji, a tylko przyspieszyła procesy które i tak były nieuniknione

Pandemia przyspieszyła i wymusiła wykorzystanie technologii

Nie powstała nowa technologia - wykorzystywano już istniejącą

Technologia jest wykosztowana jako narzędzie do utrzymania codziennego życia w "nowej normalności", nie nastąpiła głębsza przemiana wzorców zachowań.

Charakter incydentów teleinformatycznych nie uległ zmianie

Pandemia wpłynęła na przebieg cyfrowej rewolucji i znacznie ją zmieniła

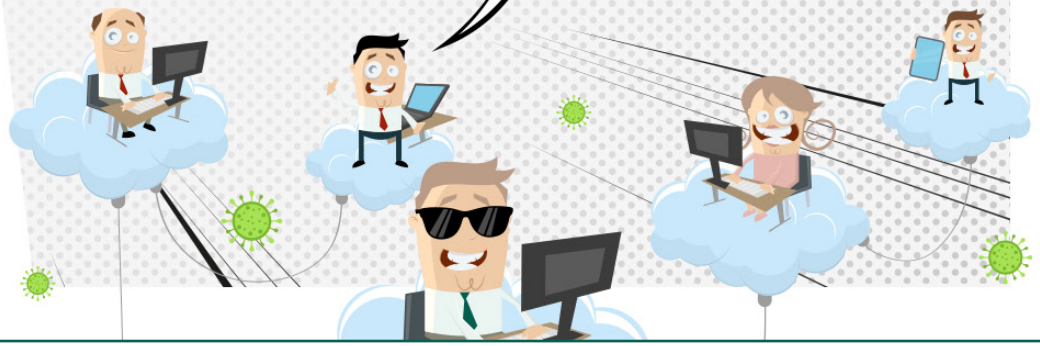
Zmienił się „mindset". Masowa praca zdalna spowodowała znaczną zmianę w sposobie myślenia i wykonywania codziennych obowiązków.

Realne wykrzywianie technologii (trwała zmiana, której nie da się już odwrócić).

Większe zrozumienie tego, jak ważnym elementem jest cyberbezpieczeństwo

Transformacja cyfrowa nie jest już „modą" ale koniecznością (wiele firm musiało przenieść działalność do sieci)

Wzrost świadomości wyzwań związanych z cyberbezpieczeństwem wśród kadry zarządczej.



seaFore 2020

Współfinansowane przez instrument
Unii Europejskiej „Łącząc Europę”