Konferencja Naukowa

DZIAŁALNOŚĆ W ZAKRESIE CYBERBEZPIECZEŃSTWA. ASPEKTY PRAWNE, ORGANIZACYJNE I TECHNICZNE

Warszawa, 7 sierpnia 2020 r., godz. 10.00-14.00

Platforma komunikacyjna PTI - MS Teams PTI

Znaczenie wyodrębnienia sektora „cyberbezpieczeństwo” dla przeciwdziałania cyberprzestępczości

Dr inż. Agnieszka Gryszczyńska, Katedra Prawa Informatycznego WPiA UKSW

W 2018 r. zespół CERT Polska przyjął **19 439 zgłoszeń** i odnotował **3 739 incydentów bezpieczeństwa**, co daje wzrost ilości incydentów o 17,5% w stosunku do 2017 r.

W 2019 r. CERT Polska zarejestrował **6 484 incydenty**.
Oznacza to lawinowy wzrost ilości incydentów – o 73 % w porównaniu z 2018 r.

Typ incydentu	Liczba incydentów	%	Liczba incydentów	%
	2018	**2018**	**2019**	**2019**
Obraźliwe i nielegalne treści	431	11,53	812	12,5
Złośliwe oprogramowanie	862	23,05	969	14,9
Gromadzenie informacji	101	2,7	95	1,5
Próby włamań	153	4,09	77	1,2
Włamania	125	3,34	160	2,5
Dostępność zasobów	49	1,31	57	0,9
Atak na bezpieczeństwo informacji	46	1,23	41	0,6
Oszustwa komputerowe	1 878	50,23	**4 086**	**63,0**
- w tym phishing	1655	44,26	3 516	54,2
Podatne usługi	69	1,85	102	1,6
Inne	25	0,67	85	1,3

Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska 2018, s. 10,
https://www.cert.pl/wp-content/uploads/2019/05/Raport_CP_2018.pdf
Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska 2019, s. 9,
https://www.cert.pl/wp-content/uploads/2020/07/Raport_CP_2019.pdf

Jaka jest skala zagrożeń?

- Od 2018 do 2019 podwoiła się ilość incydentów zarejestrowanych przez zespół CERT Polska z 3739 incydentów w 2018 r. do 6 484 incydentów w 2019 r.
- W 2018 roku phishing stanowił 44 % wszystkich incydentów.
- Zgodnie z zapowiedzią raportu CERT Polska za 2019 na 6 484 przeanalizowane incydenty stwierdzono 3 516 przypadków phishingu.

Krajobraz bezpieczeństwa polskiego internetu, Raport roczny z działalności CERT Polska 2018, s. 13, https://www.cert.pl/wp-content/uploads/2019/05/Raport_CP_2018.pdf (dostęp 20.6.2020)

- Indeks zagrożenia w Polsce wg raportu Check Point wynosi 42,7 pkt, co daje Polsce 26 miejsce w Europie i 51. na świecie
- W maju 2020 polskie przedsiębiorstwa były atakowane średnio ponad 300 razy dziennie
- Ogólna ilość cyberataków wzrosła w maju o 16% w związku z ponownym otwieraniem gospodarki.

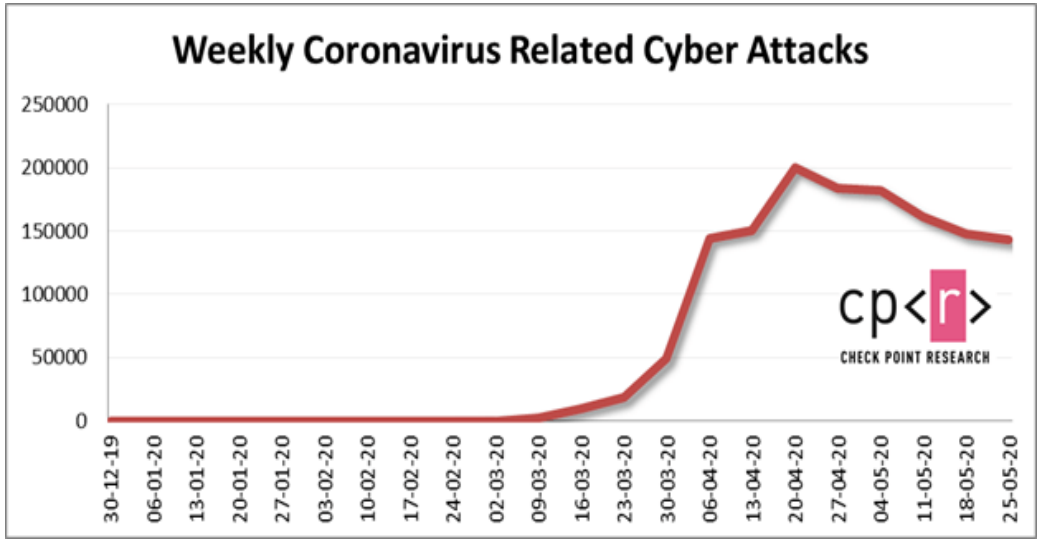
- https://www.rp.pl/CYFROWA-IT/306179901-Polska-cyberniebezpieczna-Druzgocacy-ranking.html (dostęp 20.6.2020)
- https://blog.checkpoint.com/2020/06/04/coronavirus-update-not-the-type-of-cv-youre-looking-for/(dostęp 20.6.2020)

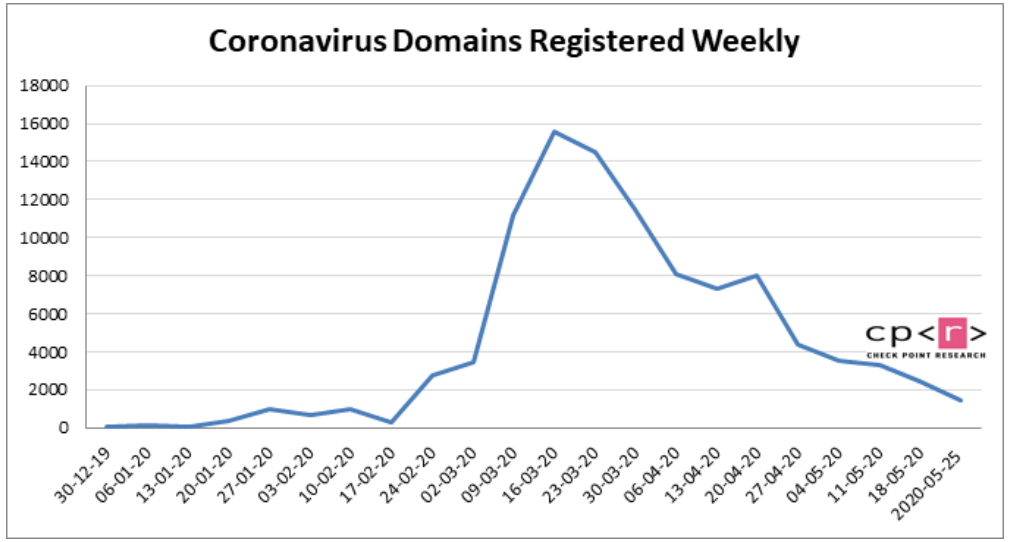
Jaka jest skala ataków związanych z COVID-19?

- W kwietniu Google zaobserwował 18 mln wiadomości phishingowych oraz złośliwego oprogramowania powiązanych z COVID-19 dziennie

https://www.theverge.com/2020/4/16/21223800/google-malware-phishing-covid-19-coronavirus-scams (dostęp 20.6.2020)

Uwagę zwraca również znaczący wzrost rejestracji domen wykorzystujących pandemię do infekowania użytkowników internetu, wyłudzania danych, środków finansowych, dezinformacji





https://blog.checkpoint.com/2020/06/04/coronavirus-update-not-the-type-of-cv-youre-looking-for/ (dostęp 20.6.2020)

Przykładowe incydenty (powiązane z COVID-19)

- Infekowanie złośliwym oprogramowaniem (głównie trojanami bankowymi) przy pomocy wiadomości e-mail zawierających złośliwe pliki imitujące CV, zwolnienia lekarskie lub dokumenty związane ze wsparciem finansowym podczas COVID-19
- Tworzenie stron fikcyjnych sklepów internetowych sprzedających środki ochronne
- Tzw. „oszustwa nigeryjskie” z wykorzystaniem w wiadomości e-mail scenariusza związanego ze wsparciem finansowym związanym z COVID-19
- Organizowanie fałszywych zbiórek pieniędzy na cele związane z ochroną zdrowia i wsparciem dla szpitali
- Tworzenie fałszywych stron agentów rozliczeniowych wyłudzających dane do logowania do bankowości elektronicznej
- Tworzenie fałszywych stron wyłudzających dane do logowania to portali społecznościowych
- Tworzenie fałszywych stron podszywających się pod WHO, Zoom, Microsoft, Google w celu wyłudzenia danych
- Infekowanie placówek ochrony zdrowia oprogramowaniem ransomware w celu wyłudzenia okupu (przykład Szpital Uniwersytecki w Brnie)

Czy dzięki COVID-19 dostrzeżono wybrane zagrożenia cyberbezpieczeństwa???

POROZUMIENIE z dnia 23 marca 2020 o współpracy w zakresie ochrony użytkowników internetu przed stronami wyłudzającymi dane, w tym dane osobowe oraz doprowadzających użytkowników internetu do niekorzystnego rozporządzenia ich środkami finansowymi w okresie stanów nadzwyczajnych, stanu epidemii lub stanu zagrożenia epidemicznego w Rzeczypospolitej Polskiej

pomiędzy
Orange Polska S.A.
Polkomtel Sp. z o.o.
P4 Sp. z o.o.
T-Mobile Polska S.A.
a
Ministrem Cyfryzacji oraz Prezesem Urzędu Komunikacji Elektronicznej (zwanymi dalej „Stroną rządową")

a także

Naukową i Akademicką Siecią Komputerową – Państwowym Instytutem Badawczym

- W okresach stanów nadzwyczajnych, stanu epidemii lub stanu zagrożenia epidemicznego w Rzeczypospolitej Polskiej, NASK-PIB będzie opracowywał, prowadził i utrzymywał jawną listę ostrzeżeń dotyczących domen internetowych, które służą do wyłudzeń danych i środków finansowych użytkowników internetu (dalej „Lista Ostrzeżeń"). Lista Ostrzeżeń jest prowadzona w formie publikacji na stronie internetowej www.cert.pl/ostrzezenia_phishing.
- Na Listę Ostrzeżeń wpisywane są domeny internetowe, które za podstawowy cel swojego działania mają wprowadzenie w błąd użytkowników internetu i w ten sposób doprowadzenie ich do niekorzystnego rozporządzenia środkami finansowymi albo do wyłudzenia ich danych osobowych
- Każdy może zgłosić domenę internetową służącą do wyłudzeń danych i środków finansowych do NASK-PIB. Zgłoszenia powinny zawierać uzasadnienie dotyczące każdej zgłoszonej domeny
- Zgłoszeń domen internetowych, o których mowa w niniejszym Porozumieniu, dokonuje się na stronie https://incydent.cert.pl/phishing lub emailem na adres: cert@cert.pl.
- Każde zgłoszenie jest weryfikowane przez NASK-PIB. NASK-PIB dołoży najwyższej staranności, aby weryfikacja zgłoszenia trwała najkrócej jak to możliwe w celu zapewniania realizacji celów niniejszego Porozumienia. Po dokonaniu weryfikacji NASK-PIB niezwłocznie wpisuje na Listę Ostrzeżeń domeny, które pozytywnie przeszły weryfikację

W dniu 20.6.2020 na liście znajdowało się 2 357 nazw domenowych, w dniu 6.8.2020 na liście znajdowało się 3 134 nazw domenowych https://hole.cert.pl/domains/domains.txt

Wybrane statystyki Listy Ostrzeżeń:

- Dla scenariusza, w którym sprawcy tworzą strony podszywające się pod agentów rozliczeniowych i banki, rejestrują nazwy domenowe podszywające się pod pocztę, podmioty świadczące usługi transportowe, rozliczeniowe i banki, na Liście Ostrzeżeń znajdują się m.in. nazwy domenowe zawierające następujące ciągi znaków:

- „poczta”
- „pay”
- „kurier”
- „dotpay”
- „paczka”
- „allegro”
- „pocztex”
- „dhl”
- „inpost”
- „platnosc”
- „payu”
- „bank”
- „dpd”
- „paczki”
- „dostawa”
- „ssl”

- Dla scenariusza, w którym sprawcy tworzą strony podszywające się pod portale informacyjne i wyłudzają dane do logowania do portali społecznościowych (zwykle kolejnym etapem jest podszywanie się pod osoby, których dane do logowania pozyskano i wysłanie próśb o pożyczenie pieniędzy poprzez wysłanie kodu BLIK), rejestrowane są głównie nazwy domenowe zawierające następujące ciągi znaków”

- „fakt”
- „porwan”
- „gwałt”
- „poszukiwan”
- „news”
- „dziennik”
- „korona”

W dniu 6.8.2020 na liście znajdowało się 1239 nazw domenowych z domeny .pl (1262 zawiera ciąg znaków „.pl”

aktywacja.allegro6.pl
aktywacja.allegro7.pl
alert-24-pl.pl
allegro.pl.sholtem.pl
allegro.pl.showltem.pl
allegro.pl.showlten.pl
allegro.pl.szoten.pl
allegro.pl-oferta.ml
allegro4.pl
allegro5.pl
allegro6.pl
allegro7.pl
allegro-blokada.pl
allegrofinanse2.pl
allegroplatnosci.pl
alleqro1.pl
arek313.civ.pl
biedronka2020x1room.p
bnpparibas-bank.pl
bok.enea-sa.pl
bok.epgnig.pl
bok.itauron.pl
bokenea.pl
bokpgnig.pl
bok-poczta.pl
bokpocztapolska.pl
bosbank-24.pl
childalertfakt.pl
cloud-sso-idea.pl
dhl-express.pl
dhl-kurier.pl
directpayment.pl
dostawa-dhl.pl
dotpay.bok-poczta.pl
dotpay.bokpocztapolska
dotpay.e-dpd.pl
dotpay.epaybylink.pl
dotpay.epocztex.pl
dotpay.e-pocztex.pl
dotpay.idpd.pl
dotpay.i-dpd.pl
dotpay.ipocztapolska.pl
dotpay.i-pocztapolska.pl
dotpay.pocztapolskasa.pl
dotpay1.pl
dotpay2.pl
dotpay3.pl
dpdpolska.pl
drogowe-akcje.ct8.pl
dworzecfakt.com.pl
dworzecfakt.pl
dworzecfakt.waw.pl
dworzeconline24.com.pl
dworzeconline24.pl
dworzeconline24.waw.pl
dworzecporwanie.pl
dworzecporwaniepl.com.pl
dworzecporwaniepl.net.pl
dworzecporwaniepl.pl
dworzecporwaniepl.waw.pl
dworzecporwaniepl-24.pl
dzieckoalert.com.pl
dzieckoalert.net.pl
dzieckoalert.pl
dzieckoalert.waw.pl
dziennewiadomosci24.pl
dziennikgminny.098.pl
dziennikgminny.h2g.pl
dziennikinformacyjny.098.pl
dziennikinformacyjny.h2g.pl
dziennikmiasto.098.pl
dzienniknews.com.pl
dzienniknews.pl
dziennikpolska.h2g.pl
dziennikpolski.098.pl
dziennikpolski.hekko24.pl
dziennikswiat.hekko24.pl
emonitoring.poczta-polska2.pl
emonitoring.poczta-polska4.pl
emonitoring.poczta-polska8.pl
emonitoring24.net.pl
energabok.pl
enewsgwalt24.pl
e-newsgwalt24.pl
enpgnig.pl
e-osobyzagionione.pl
epaybylink.pl
epayu.pl
epge-bok.pl
epity2020.pl
e-pity-2020.pl
epocztapolska.pl
epocztapolska24.pl
epocztex.pl
e-pocztex.pl
e-polskaporwania.pl
epolskaporwanie.pl
e-polskaporwanie.pl
e-pomagajmypl.pl
e-porwaniapolska.pl
eporwaniedziecka.com.pl
eporwaniedziecka.net.pl
eporwaniedziecka.pl
eporwaniedziecka.waw.pl
eporwanienatalki.pl
e-porwanienatalki.pl
eporwaniepolska.pl
e-porwaniepolska.pl
eporwaniepolska48.pl
e-porwaniepolska48.pl
eposzukiwananatalka.pl
e-poszukiwananatalka.pl
e-poszukiwania.com.pl
e-poszukiwania.pl
e-poszukiwanialaury.pl
e-poszukiwanie.pl
euprowadzeniedworzec.pl
e-uprowadzeniedworzec.pl
pgnig-24.pl
pgnigonline.pl
pilnasprawa.hekko24.pl
pilnesprawy.h2g.pl
platnosciallegro.pl
plikgier.5p.pl
pl-pl-fb.pl
poczta-polska3.pl
poczta-polska4.pl
poczta-polska5.pl
poczta-polska6.pl
pocztex24.pl
polaczenie.xn.pl
policja24info.pl.d103wh.d2.cz
polskapolicja24.pl.d214wh.d2.cz
polskaporwania.com.pl
polskaporwania.net.pl
polskaporwania.pl
polskaporwanie.com.pl
polskaporwanie.net.pl
polskaporwanie.pl
polskidziennik.098.pl
polskidziennik.pl
polskiewiadomosci.098.pl
pomagajmypl.net.pl
pomagajmypl.pl
pomagamszukac.098.pl
pomagamy-fakty24.pl
pomoc-fakty24.pl
portalgminny.cal24.pl
portalibrus.pl
portalinformacyjny.098.pl
portalinformacyjny.h2g.pl
portalpowiatowy.098.pl
portalpowiatowy.cal24.pl
portalsasiedzki.098.pl
portalsasiedzki.h2g.pl
portalwojewodzki.098.pl
portalwojewodzki.cal24.pl
porwania.pl
porwaniadzieci.com.pl
www.aktywacja.allegro6.pl
www.alert-24-pl.pl
www.allegro.pl.sholtem.pl
www.allegro.pl.showlten.pl
www.allegro.pl.szoten.pl
www.allegro4.pl
www.allegro5.pl
www.allegro6.pl
www.allegro7.pl
www.allegro-blokada.pl
www.alleqro1.pl
www.arek313.civ.pl
www.biedronka2020x1room.pl
www.bnpparibas-bank.pl
www.bok.enea-sa.pl
www.bok.epgnig.pl
www.bok.itauron.pl
www.bokenea.pl
www.childalertfakt.pl
www.dhl-express.pl
www.dostawa-dhl.pl
www.drogowe-akcje.ct8.pl
www.dworzecfakt.com.pl
www.dworzecfakt.pl
www.dworzecfakt.waw.pl
www.dworzeconline24.com.pl
www.dworzeconline24.pl
www.dworzeconline24.waw.pl
www.dworzecporwanie.pl
www.dworzecporwaniepl.com.pl
www.dworzecporwaniepl.net.pl
www.dworzecporwaniepl.pl
www.dworzecporwaniepl.waw.pl
www.dworzecporwaniepl-24.pl
www.dzieckoalert.com.pl
www.dzieckoalert.pl
www.dzieckoalert.waw.pl
www.dziennewiadomosci24.pl
www.dziennikgminny.098.pl
www.dziennikgminny.h2g.pl
www.dziennikinformacyjny.098.pl
www.dziennikinformacyjny.h2g.pl

8 nazw domenowych z listy zawierało ciąg znaków „gov”

gov-24.com
gov-warszawa.pl
warszawa-gov.pl
warszawa-gov24.pl
www.gov-24.com
www.gov-warszawa.pl
www.warszawa-gov.pl
www.warszawa-gov24.pl

6 z powyższych nazw domenowych zawierających ciąg „gov” jest z domeny .pl

Problemy

- Brak powszechnej świadomości zagrożeń i ich skutków
- Brak świadomości zagrożeń i ich skutków u decydentów (w tym osób odpowiedzialnych za tworzenie, wykonywanie i przestrzeganie przepisów prawnych), osób odpowiadających za budżety (podmiotach publicznych i prywatnych)
- Brak wiedzy na temat wektorów ataków, sposobów zabezpieczeń, działań niezbędnych do podjęcia w sytuacji incydentu
- Brak wiedzy na temat cyberbezpieczeństwa, cyberprzestępczości i jej zwalczania po stronie podmiotów decydujących o treści przepisów prawnych

- Cyberbezpieczeństwo nie jest priorytetem działań podmiotów publicznych i prywatnych
- Zwalczanie cyberprzestępczości nie jest priorytetem organów ścigania (poza tym cyberprzestępczości „nie widać” w statystykach)

- Brak powszechnych i specjalistycznych szkoleń z zakresu cyberbezpieczeństwa czy brak potrzeby podnoszenia poziomu wiedzy i umiejętności z zakresu cyberbezpieczeństwa?
- Brak specjalistów na rynku?
- Brak środków finansowych na cyberbezpieczeństwo

- **Mała ilość podmiotów wyspecjalizowanych, dla których cyberbezpieczeństwo to podstawowy przedmiot działalności**

Co ułatwia sprawcom ataki i utrudnia ustalenie ich tożsamości?

- Możliwość anonimowego korzystanie z usług świadczonych drogą elektroniczną
- Wykorzystanie tożsamości innych osób (z uwagi na brak weryfikacji tożsamości przy korzystaniu z e-usług)
- Ograniczenie zakresu danych publikowanych w bazach WHOIS – utrudniające m.in. atrybucje ataku oraz prowadzenie postępowań karnych
- Obrót zarejestrowanymi na dane innych osób kartami SIM
- Brak przepisów regulujących gromadzenie logów, ich struktury oraz ustalenia okresu ich przechowywania
- Brak retencji danych „internetowych” – w szczególności w zakresie logów oraz danych abonentów usług
- Stosowanie NAT w sieciach (przy jednoczesnym niegromadzeniu przez większość podmiotów -w tym banki numerów portów)
- Łatwość pozyskania rachunków bankowych do prania pieniędzy pochodzących z przestępstwa
- Dostępność anonimowych usług płatniczych (płatności w kryptowalucie, płatności przy pomocy SMS Premium)
- Brak ogólnych regulacji dotyczących blokowania domen podszywających się pod inne podmioty lub służących do popełnienia przestępstwa
- Wadliwa regulacja karnoprawnych znamion kradzieży tożsamości
- Bardzo niskie zagrożenie karne przestępstwa „hackingu”

Postulaty *de lege ferenda*

- Celowe jest wprowadzenie obowiązków związanych z przechowywaniem logów dostępowych oraz danych abonentów usług świadczonych drogą elektroniczną przez okres 12 miesięcy (retencja danych).

- Dla podniesienia poziomu bezpieczeństwa i przeciwdziałania zjawisku kradzieży tożsamości celowe jest wprowadzenie obowiązków dotyczących lepszej weryfikacji tożsamości podmiotów korzystających z usług podmiotów świadczących usługi drogą elektroniczną.

- Z uwagi na to, że w części z omówionych powyżej ataków wykorzystano nazwy domenowe z domeny *.pl lub domeny gdzie rejestratorami (pośrednikami) są podmioty mające siedzibę na terytorium Polski należy dokonać zmian w procesie pośrednictwa w rejestracji domen i nałożyć na rejestratorów obowiązki związane z weryfikacją tożsamości podmiotów rejestrujących domeny (abonentów).

- Jawny rejestr domeny .pl powinien zawierać dane kontaktowe do abonenta domeny (co najmniej adres e-mail). Aktualnie w bazie WHOIS nie są publikowane dane abonentów będących osobami fizycznymi. Dla porównania należy wskazać, że dla domeny *.eu baza WHOIS zawiera dane w postaci adresu mailowego abonenta.

- Celowe jest wprowadzenie w sytuacji nabycia karty przedpłaconej (SIM) od innego podmiotu obowiązku ponownej rejestracji takiej karty pod rygorem dezaktywacji usługi. Aktualna regulacja w zestawieniu z praktyką pokazuje, że cel wprowadzenia rejestracji abonentów usług przedpłaconych ustawą o działaniach antyterrorystycznych nie został osiągnięty, a zarejestrowane na dane innych osób karty SIM można kupić na powszechnie dostępnych portalach ogłoszeniowych oraz na forach w sieci TOR.

- Celowe jest dalsze prowadzenie Listy Ostrzeżeń, należy jednak jej dalsze prowadzenie oprzeć o przepisy prawa powszechnie obowiązującego i wprowadzić procedurę odwoławczą.

- **Art. 279.** § 1 kk

- Kto kradnie z włamaniem, podlega karze pozbawienia wolności od roku do lat 10.

- **Art. 267. § 1 kk**

- Kto bez uprawnienia **uzyskuje dostęp do informacji dla niego nieprzeznaczonej**, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub **przełamując albo omijając** elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności **do lat 2.**

Mając na względzie skalę oraz skutki ataków niezbędne jest również podniesienie górnej granicy odpowiedzialności karnej za czyn z art. 267 § 1 kk.
Aktualne zagrożenie karne wynosi do 2 lat pozbawienia wolności!!!!

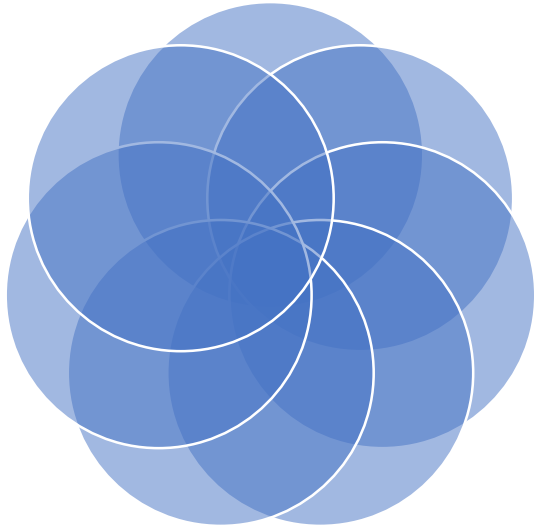
Czy wyodrębnienia sektora „cyberbezpieczeństwo” ma znaczenie dla przeciwdziałania cyberprzestępczości?

SOC

Analizy danych

Powszechne szkolenia

Powszechne szkolenia



Zabezpieczanie danych

Zwiększenie odporności na cyberataki w podmiotach prywatnych

Badanie zabezpieczonych nośników

Analiza logów

CSIRT sektorowe

Racjonalizacja wydatkowania środków na cyberbezpieczeństwo

Thret hunting

Thret intelligence

Dziękuję za uwagę!

Kontakt: a.gryszczynska@uksw.edu.pl