## Sytuacje, na jakie można się natknąć, w związku z trwającą pandemią wirusa SARS-coV-2

Okres izolacji społecznej wymusił zmiany w codziennym życiu praktycznie dla każdego. Bardzo dużo aspektów związanych z zaspokajaniem nawet elementarnych potrzeb, tam gdzie było to możliwe, zaczęło być realizowanych w przestrzeni wirtualnej. Obowiązkowe zdalne nauczanie, praca zdalna wszędzie tam, gdzie tylko jest ona możliwa, zakupy w sklepach internetowych – to tylko przykłady zmian, do których natychmiast dostosowali się cyberprzestępcy.

Znane są przypadki infekowania komputera domowego przez nieświadome dziecko próbujące połączyć się do wirtualnych zajęć za pomocą zmodyfikowanych przez hackerów linków.

Warto dokonać przeglądu zabezpieczeń naszych domowych komputerów, routerów. Zakupić, jeśli nie posiadamy i zainstalować narzędzia z grupy „Internet security" (zapora sieciowa, pakiet antywirusowy, antyspamowy) lub skorzystać z choćby, darmowych narzędzi antywirusowych.

Warto też, jeśli nie mamy kopii zapasowej, wykonać tzw. backup istotnych danych na zewnętrzny dysk USB, domowy dysk sieciowy lub skorzystać z rozwiązań w tzw. „chmurze".

Bardzo często cyberprzestępcy wykorzystują tematy ważne społecznie, aby wyłudzić dane od osób, którym zależy na wiedzy związanej z tym zagadnieniem – w tym wypadku z panujących stanem zagrożenia epidemicznego. Towarzyszą temu skrajne emocje: aktualnie wiążą się z one koronawirusem i z lękiem przed tym zakażeniem. Nośny medialnie tytuł, zacytowana wypowiedź eksperta czy nagranie wideo związane z tematem, mogą skutecznie uśpić czujność. Hakerzy wysyłają również maile z linkami do stron, na których można zakupić leki na COVID-19. To jest oczywistą dezinformacją, ponieważ taki lek w tym momencie jeszcze nie istnieje. W sytuacjach stresowych ludzie często nie myślą logicznie i nie sprawdzą skąd pochodzi dana informacja. Cyberprzestępca tworzy typowy „fake news", której celem jest np. podanie swoich danych do zalogowania się w serwisie społecznościowym, lub kliknięcia w dany link. Często pod takim linkiem kryją się wymuszenia podania danych do wykonania przelewu (np. zbiórka na leczenie osoby zakażonej koronawirusem). W innych przypadkach po wejściu na link, nasz sprzęt zostaje zainfekowany.

Na stronach internetowych Ministerstwa Cyfryzacji znajdują się informacje na temat blokowania oszustów wykorzystujących pandemię do własnych celów. Podejrzane domeny będą podane do publicznej wiadomości. W szeregu przypadkach będą kierowane powiadomieni na policję i do prokuratury. Działanie te są efektem współpracy rządu z operatorami telekomunikacyjnymi.

Zaleca się:

- Być ostrożnym w przypadku ogłoszeń dotyczących leków na COVID-19, zwłaszcza ich sprzedaży;
- Uważać na organizowane prywatne zbiórki środków na walkę z COVID-19;
- Korzystać ze sprawdzonych i wiarygodnych portali zakupowych i aukcyjnych;
- Aby weryfikować adresy stron, które proszą o kliknięcie w link i podanie swoich danych, haseł, loginów;
- Nie odpowiadać na podejrzane SMSy związane z odbiorem przesyłką kurierską i epidemią;
- Dokładnie analizować treść umów i regulaminów transakcji zawieranych przez Internet;
- Wnikliwie przestudiować przed podpisem oferty kredytowe, szczególnie w przypadku bardzo "atrakcyjnych" warunków;
- Sprawdzać, czy interesująca nas strona posiada certyfikat SSL (szczególnie w przypadku banków);
- Sprawdzać informacje w wiarygodnych źródłach, np. strony gov.pl;
- Przekazać i tłumaczyć powyższe informacje starszym osobom w rodzinie (i poza nią).

Jeśli chodzi o zdalną pracę to bardzo szybko okazało się, że infrastruktura informatyczna większości firm nie jest przygotowana na długotrwałe jej funkcjonowanie, co często skutkowało problemami z połączeniami oraz komunikatami o błędach. Spora część tych błędów, jak pokazują raporty, to efekt błędów ludzkich, omijania procedur, zainfekowania komputerów. Kwarantanna to wyzwanie dla firm, które w błyskawicznym tempie musiały przestawić się ze spotkań osobistych na telekonferencje i masowe wykorzystanie komunikatorów. Z dnia na dzień uległ zmianie styl pracy, lecz nie zawsze nadążyły za tym zmiany w dziedzinie zapewnienia bezpieczeństwa sieciowego i odpowiedniego przeszkolenia pracowników.

Na porządku dziennym występują próby wyłudzenia informacji, masowe kampanie phishingowe oraz ataki typu ransomware.

W warunkach stresu związanego z sytuacją izolacji społecznej często dochodzi do wykonywania przez pracowników pochopnych działań i podejmowania złych decyzji.

Aby uchronić się przez atakiem należy:

- bezwzględnie stosować się do procedur bezpieczeństwa jakie obowiązują u naszego pracodawcy;
- przekazywać do działów bezpieczeństwa i działu IT wszelkie zaobserwowane; nieprawidłowości w działaniu sprzętu i oprogramowania oraz inne podejrzane sytuacje;
- uruchamiać regularny skanowanie antywirusowe oraz instalować uaktualnienia zabezpieczeń,
- nie klikać podejrzanych linków na stronach WWW lub w otrzymanych wiadomościach e-mail/ SMS oraz nie otwierać żadnych załączników co do którym mamy jakąkolwiek wątpliwość odnośnie ich wiarygodności.

Mimo luzowania przez Rząd obostrzeń wprowadzonych na czas pandemii należy być bardzo ostrożnym zarówno w

przestrzeni wirtualnej jak i tej rzeczywistej. Wszystkim życzymy dużo zdrowia i cierpliwego znoszenia ograniczeń!

**Informacji z cyklu zagrożeń z dziedziny cyberbezpieczeństwa opisuje sytuacje z jakimi można się obecnie spotkać w związku z wybuchem pandemii wirusa SARS-coV-2.**

Przede wszystkim podkreślić należy fakt, że każda sytuacja może zostać wykorzystana do tego, aby przeprowadzić atak, dokonać oszustwa, wyłudzenia czy w jakikolwiek inny nieetyczny sposób osiągnąć zysk. Obecnie działania cyberprzestępców wykorzystują naturalne ludzkie odruchy i emocje:  strach, stres, atmosferę niepewności i zagrożenia.

Bardzo dużo osób otrzymało ostatnio wiadomości SMS lub e-mail informujące o tym, że planowane są działania państwa polegające na zajęciu środków zdeponowanych w bankach na poczet walki z koronawirusem. Celem zachowania pewnych sum na kontach bankowych proponuje się złożyć odpowiednią deklarację, dostępną na stronie, do której odsyła załączony link. **Pod żadnym pozorem nie należy otwierać takiego linku!**

Należy również zwrócić szczególną uwagę na komunikaty otrzymywane droga mailową z naszych banków czy innych instytucji. Niektóre z nich to spreparowane wiadomości typu phishing w których oszuści, wykorzystując panującą sytuację i podszywając się pod znane nam podmioty, informują o swoich działaniach związanych z sytuacja epidemiczną. Szczegóły są dostępne w załączonych linkach, których otwarcie kieruje na spreparowane strony wyłudzające dane. Należy zachować szczególną ostrożność w takich sytuacjach i weryfikować czy strona posiada stosowne zabezpieczenia.

Rozpaczliwa sytuacja szpitali proszących o pomoc materialną wykorzystywana jest przez oszustów tworzących w Internecie fikcyjne zbiórki pieniędzy na zakup środków ochrony osobistej. **Przed wpłatą należy upewnić się kto jest organizatorem zbiórki**, czy jest to zaufana, powszechnie znana instytucja.

Problemy w zaopatrzeniu w środki ochrony osobistej stały się polem do nadużyć i oszustw. Pojawiły się w Internecie oferty sprzedaży masek, środków dezynfekujących, rękawiczek i itp. w spekulacyjnych cenach. Duże portale aukcyjne rozpoczęły walkę z tego typu praktykami, ale wciąż można natrafić na tego typu ogłoszenia.

Pojawiły się również oferty sprzedaży medykamentów, leków i innych środków reklamowanych jako skuteczne w profilaktyce lub walce z wirusem, podpierające się często pseudonaukowymi opiniami lub dowodami skuteczności. **Należy pamiętać, że wciąż nie ma oficjalnie zalecanych i zatwierdzonych  leków ani szczepionki na wirusa SARS-coV-2.** Zakup tego typu środków nie zabezpieczy przed wirusem, a może wręcz doprowadzić do problemów zdrowotnych.Można również dotrzeć do ofert sprzedaży testów na obecność koronawirusa z niepewnych i niesprawdzonych źródeł (najczęściej azjatyckich) – tu również apeluje się o daleko idącą ostrożność i rozwagę!

Obowiązujące rozporządzenia i kampania medialna zachęcająca do pozostania w domu powoduje, że wzrosła sprzedaż przez Internet. To również pole do ogromnych nadużyć i oszustw. Pojawia się sporo fikcyjnych sklepów kuszących rabatami, promocjami i atrakcyjnymi ofertami odwołując się do haseł #zostanwdomu. Przypominamy, że należy upewnić się czy e-sklep, w którym znaleźliśmy coś interesującego jest wiarygodny.

Przypominamy, że aktualne informacje na temat koronawirusa dostępne są pod adresem https://www.gov.pl/web/koronawirus.

Polecamy również naszą stronę intranetową:https://ipk.gkpge.pl/aktualnosci/Strony/Koronawirus.aspx

**Zagrożenia na jakie jesteśmy narażeni, gdy decydujemy się na podłączenie do otwartych sieci WiFi.**

Stały dostęp do internetu okazuje się obecnie wręcz niezbędny do funkcjonowania, przynajmniej dla przeważającej części społeczeństwa. Bycie "on-line" stało się modą, stylem życia, w wielu przypadkach sposobem na prowadzenie własnego biznesu. Wiele osób nie jest w stanie wyobrazić sobie życia bez smartfonu, tabletu, laptopa w domu i poza nim. Jedno z pierwszych pytań jakie pada gdy pojawiamy się w nowym miejscu brzmi: "Czy jest tu jakieś WiFi ?". Wiadomo, pakiety internetowe w smartfonach są obecnie czymś normalnym, ale tez mają ograniczoną wielkość i bardzo chętnie tam gdzie się da chciałoby się oszczędzić - stąd darmowe WiFi brzmi często jak ocalenie. Zwłaszcza za granicą, na wakacjach, na lotnisku, w hotelu czy w restauracji. Wrzucenie doskonałego zdjęcia na Facebooka lub Instagrama "kosztuje" wtedy mniej. Ale czy aby na pewno ?

Nie wszyscy bowiem zdają sobie sprawę, jak niebezpieczne może być korzystanie z hotspotów - publicznie udostępnionych sieci bezprzewodowych. Zastanówmy się na czym polega zagrożenie?

Publicznie dostępne sieci bardzo rzadko są zabezpieczone równie dobrze co siec biurowa czy domowa, a zdarza się, że tych zabezpieczeń nie posiadają praktycznie wcale. Tym samym stanowią bardzo wygodną, prostą i skuteczną furtkę dla różnego rodzaju cyberprzestępców mogących bez wysiłku wykraść nasze dane, prywatne hasła czy inne informacje. Dlaczego tak jest?W przypadku sieci domowych nazwa sieci (SSID) wraz z hasłem (najczęściej stosunkowo skomplikowanym - chcemy się w końcu chronić przed sąsiadami), oraz w połączeniu z protokołem szyfrowania (np. WPA /WPA2) tworzy bezpieczną enklawę. W centrum handlowym, kawiarni czy w parku widzimy bardzo często tylko nazwę dostępnej otwartej sieci. Wystarczy tylko kliknąć i być online.

Jeśli to zrobimy - wszystko to co piszemy na laptopie lub smartfonie, zaczyna krążyć po sieci w postaci niezaszyfrowanej:

treści na komunikatorze, numery karty kredytowej, hasło do poczty elektronicznej - czy można być bardziej wymarzonym "klientem" dla cyberprzestępcy?

A stąd już prosta droga do utraty pieniędzy na koncie, czy kradzieży tożsamości - wirtualne zagrożenie może szybko przerodzić się w realne problemy.

Jak więc bezpiecznie korzystać z internetu poza domem łącząc się z hotspotami? Trzeba przestrzegać kilku podstawowych zasad.

- Traktuj każdą nieznaną sieć jako podejrzaną. Zweryfikuj jej nazwę z danymi uzyskanymi np. od obsługi hotelu, kelnera w kawiarni, czy personelu lotniska.
- Unikaj sieci niechronionych hasłem. Są one najbardziej podejrzane, często są celowo generowane przez hackerów by skusić potencjalne ofiary do podłączenia się do nich.
- Wyłącz automatyczne łączenie się z sieciami bezprzewodowymi. Mimo, iż ucierpi na tym Twoja wygoda, to Ty zdecydujesz czy sieć, w zasiągu której właśnie się znalazłeś, jest bezpieczna.
- Korzystaj z programu antywirusowego i zapory. Mimo iż to podstawa, wciąż nie każdy o tym pamięta i nie korzysta nawet z dostępnych darmowych rozwiązań.
- Planując wykonanie operacji bankowych, płatności kartą przełącz się na transfer danych w telefonie i upewnij się czy łączysz się z właściwym serwisem, stosującym protokół SSL. Bezpieczna strona oznaczona będzie zieloną kłódką a w jej adresie znajdzie się "https" zamiast "http"
- Jeżeli planujesz połączyć się z domowym serwerem, lub siecią firmową koniecznie skorzystaj z mechanizmu VPN - Virtual Private Network, tworząc wirtualny, szyfrowany tunel zapewniający bezpieczne połączenie. Można go w prosty sposób utworzyć korzystając nawet z darmowych aplikacji.
- Jeśli to możliwe tam, gdzie wprowadzasz hasła, postaraj się wprowadzić dwustopniowy proces uwierzytelniania, np. poprzez weryfikację danych SMS-em. Zadbaj też o to by hasła te były bezpieczne.

Na koniec odrobina statystyki. W 2016 roku,wg danych firmy Symantec , z publicznych sieci korzystało aż 87% amerykańskich konsumentów, a ponad 60% z nich uważało, że nie ma w tym żadnego niebezpieczeństwa. Pozostaje mieć nadzieję, że polscy internauci, oraz ta publikacja, poprawi te wyniki.

## Informacja dotycząca zagrożeń podczas zakupów w sklepach elektronicznych

Kolejna porcja informacji z cyklu zagrożeń z dziedziny cyberbezpieczeństwa dotyczy zagrożeń na jakie jesteśmy narażeni podczas gorączkowych zakupów przedświątecznych dokonywanych coraz częściej za pomocą sklepów elektronicznych.

Boże Narodzenie to czas, które zwyczajowo spędzamy w rodzinnym gronie, pośród bliskich, których dodatkowo chcemy obdarować prezentami. Chcąc uniknąć zatłoczonych sklepów, galerii, parkingów coraz częściej uwagę naszą przykuwa oferta internetowych sklepów oferujących relatywnie tani i bogaty asortyment w zasadzie wszystkiego co tylko chcemy kupić.

Badania wskazują, że już 62% zakupów w Polsce dokonywanych jest w internecie. Niestety wyniki badań analizują również przestępcy i bardzo skrzętnie wykorzystują nasze preferencje, podszywając się pod sklepy online, operatorów płatności lub zamieszczając fałszywe ogłoszenia i oferty.

Świadomość zagrożeń jakie czyhają na nas po przekroczeniu progu wirtualnego sklepu pozwoli uniknąć przykrych niespodzianek.

- Warto zacząć od weryfikacji, jak długo działa e-sklep, który nas interesuje - im dłużej funkcjonuje na rynku, tym często większe bezpieczeństwo naszych zakupów. Czujność powinny wzbudzać szczególnie kuszące oferty oferowane przez nieznanych dostawców.
- Koniecznie przeczytajmy opinie o sklepie czy sprzedawcy, które publikowane są w internecie. Szczególną ostrożność powinny wzbudzić te, które posiadają wiele negatywnych komentarzy wystawionych w krótkim czasie. Często można natychmiast dowiedzieć się, że sklep, który kusi nas doskonałą ofertą jest atrapą, która zniknie z naszych oczu natychmiast po dokonaniu płatności.
- Sprawdź dane kontaktowe na stronie sklepu, poszukaj adresu siedziby, numeru telefonu kontaktowego, bądź ostrożny jeśli sklep oferuje wyłącznie możliwość kontaktu elektronicznego. Wiarygodny sklep podaje dane rejestrowe (NIP, KRS, REGON), które można zweryfikować w ogólnodostępnych rejestrach.
- Uważaj na tzw. "wyjątkowe okazje" gdyż przestępcy stosują metodę zwabiania ofiar wyjątkowo korzystnymi ofertami na przedmioty kosztujące zazwyczaj znacznie więcej.
- Sklep oferujący możliwość odbioru osobistego jest bardziej wiarygodny od tego, który taką możliwość wyklucza.
- Przystępując do płatności, sprawdź czy zostałeś skierowany do prawdziwej strony operatora płatności lub banku. Sprawdź czy nazwa domeny jest prawidłowa i czy ma certyfikat bezpieczeństwa SSL widoczny na pasku adresowym w przeglądarce.
- Korzystaj z usług zaufanych i uznanych na rynku operatorów. Twój niepokój powinno wzbudzić żądanie podania danych z karty płatniczej na stronie bliżej nieznanego sklepu bez możliwości wyboru innego rodzaju płatności.
- Zwracaj uwagę na to czy informacje na stronie, na której masz dokonać płatności, są sformułowane prawidłowo, logicznie, poprawnie gramatycznie i ortograficznie. Wszelkie błędy winny wzbudzić twój uzasadniony niepokój ponieważ legalny i profesjonalny sklep dba o każdy szczegół.
- W przypadku korzystania z zagranicznych sklepów, upewnij się w jakiej walucie jest podana cena. Zdarza się, że na stronie produktu jest ona pokazywana w złotówkach a na stronie płatności w dolarach lub euro.

- Unikaj korzystania z linków do płatności przesłanych w wiadomościach SMS, które bardzo często prowadzą do fałszywych stron operatorów płatności lub banków.
- W razie wątpliwości skontaktuj się ze sklepem i zażądaj wyjaśnień. W przypadku problemów z uzyskaniem kontaktu odstąp od takiej transakcji i poszukaj alternatywnego źródła.
- Bądź czujny jeśli sklep przy składaniu zamówienia żąda od Ciebie podania nadmiarowych informacji - może być to próba pozyskania Twoich poufnych danych, których utrata może narazić Cię na dotkliwe straty.
- Jeśli masz podejrzenia, że sklep może być instytucją fałszywą, lub już podałeś dane do swojej karty, skontaktuj się niezwłocznie z Twoim bankiem w celu zablokowania karty oraz zgłoś sprawę na Policję.

Święta to czas radości, którą chcemy dzielić z bliskimi. Zadbajmy, o to by chwila nieuwagi, lub nieprzemyślana decyzja nie wpłynęła na nasz nastrój. Życzymy udanych i bezpiecznych zakupów, ale nade wszystko spokojnych, radosnych oraz pełnych ciepła i pozytywnej energii Świąt Bożego Narodzenia.

## Informacje z cyklu zagrożeń z dziedziny cyberbezpieczeństwa - hasła

Historycznie często stosowano tajny ciąg słów lub zdań by w ten sposób osoba je wypowiadająca mogła się uwierzytelnić. Pamiętamy słynne "Najlepsze kasztany rosną na placu Pigalle" które w połączeniu z odzewem "Zuzanna lubi je tylko jesienią" i kontrodzewem "Przesyła Ci świeżą partię" w słynnym polskim filmie sprawiało, że nieznajomi ludzie zaczynali sobie ufać. Obecnie również stosuje się tę metodę w sytuacji kiedy chcemy sprawić, aby jakiś system teleinformatyczny nam zaufał i uznał, że może nas dopuścić do informacji które ma prawo właśnie nam udostępnić. Zazwyczaj w tym celu stosuje się kombinację identyfikatora o skojarzonego z nim hasła. Musimy przedstawić się, zidentyfikować się, podając np. *login_name* do konta pocztowego aby następnie po podaniu *hasła* dokonać tzw. autentykacji.

Zazwyczaj hasło stanowi ciąg znaków o określonej minimalnej liczbie, składający się z kombinacji małych i dużych liter, cyfr oraz tzw. znaków specjalnych np. !@#$%&.,)(.

To jak bardzo skomplikowane i trudne do odgadnięcia (złamania, przejęcia) jest hasło przekłada się wprost na bezpieczeństwo danych, do których para *identyfikator-hasło* broni dostępu.

Musimy mieć świadomość, że przestępcy chcący wejść w posiadanie naszych informacji lub pieniędzy, dzięki coraz to potężniejszej mocy obliczeniowej popularnych komputerów, dysponują coraz to skuteczniejszymi metodami łamania haseł. Do niedawna za bezpieczne uważano hasła składające się z 8 znaków, teraz zaleca się aby miały już minimum 10 albo wręcz 12 - a każdy znak więcej zwiększa bezpieczeństwo.  Na złamanie hasła składającego się z 8 znaków potrzeba obecnie mniej niż 8 h, zaś 12 znakowego ok 1 roku. To tłumaczy dlaczego jesteśmy wciąż zachęcani do częstego zmieniania hasła.

## Informacje z cyklu zagrożeń z dziedziny cyberbezpieczeństwa - tzw. phishing

Phishing jest metodą oszustwa, w której przestępca podszywa się pod inną osobę, lub instytucję w celu wyłudzenia wrażliwych danych należących do użytkownika (takich jak np. dane logowania, hasła, numery konta bankowego lub karty kredytowej), lub nakłonienia ofiary do wykonania określonych działań. Atak ten jest oparty na metodach inżynierii społecznej i wykorzystuje naturalną cechę człowieka jaką jest zaufanie. Atakujący podszywa się bowiem pod legalnie działające organizacje, instytucje, agencje rządowe czy dostawców usług z którymi na co dzień jesteśmy w stałym kontakcie. Doskonale przygotowane zarówno pod względem graficznym jak i treści wiadomości e-mail, w sposób grzeczny i przekonywujący informują o konieczności kontaktu w celu np. potwierdzenia informacji, uzupełnienia danych koniecznych do kontynuacji współpracy, uregulowania powstałej drobnej różnicy w płatnościach, często informują o doskonałej krótkookresowej ofercie sklepu on-line lub o pewnych problemach, których rozwiązanie wymaga zalogowania się do systemu. Do wiadomości najczęściej dołączony jest link, który przekierowuje ofiarę ataku do fałszywej strony na której dochodzi albo do kradzieży tożsamości, albo do zainfekowania urządzenia z którego ta osoba korzysta w celu późniejszej penetracji systemu komputerowego i kradzieży danych. Tego typu ataki są przygotowywane na coraz wyższym poziomie, dlatego trudno jest odróżnić prawdziwą wiadomość od wiadomości phishingowej.

Jak więc rozpoznać phishing? Czujność naszą powinny wzbudzać każde wiadomości i komunikaty z prośbą o ujawnienie osobistych i poufnych informacji za pośrednictwem poczty elektronicznej lub stron internetowych.

Jak można się ochronić przed takim atakiem?

- Miej dobre nawyki i nie reaguj na linki w niechcianych wiadomościach e-mail, pochodzących od nieznanych Ci osób lub instytucji oraz na portalach społecznościowych.
- Nigdy nie otwieraj załączników w takich wiadomościach
- Dokładnie sprawdzaj adres strony. Często strony są doskonale spreparowane i sprawiają wrażenie poprawnych, ale adres URL mają inny niż oryginalny adres instytucji (np. inna domena)
- Nigdy nie ujawniaj nikomu swojego hasła. Tego typu prośba powinna zawsze wzbudzić podejrzenie!
- Nie przekazuj nikomu poufnych danych - przez telefon, osobiście ani przez e-mail lub stronę internetową.
- Dbaj o to by korzystać z legalnego oprogramowania, z aktualnej wersji przeglądarki, instalują najnowsze poprawki zabezpieczeń.
- Korzystaj z oprogramowania antywirusowego, szereg producentów posiada narzędzia do ochrony przed phishingiem.

## Informacje z cyklu zagrożeń z dziedziny cyberbezpieczeństwa - programy antywirusowe

Podstawowym i najważniejszym narzędziem ochrony naszych urządzeń, komputerów, laptopów, tabletów czy telefonów komórkowych oraz danych na nich zawartych są programy antywirusowe, które muszą być regularnie uaktualniane. Już nawet powszechnie dostępne, darmowe wersje systemów antywirusowych, wielokrotnie zwiększają poziom zabezpieczenia naszych urządzeń przed penetracją złośliwego oprogramowania mogącego skutecznie zniszczyć nasze dane. Już dzisiaj sprawdź więc czy Twój laptop, tablet czy telefon komórkowy ma zainstalowany program antywirusowy z aktualną bazą wirusów.

**Realizując postanowienia Ustawy z dnia 5 lipca 2018 o Krajowym Systemie Cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560, zwanej dalej "UKSC"), na mocy której Minister Energii wydał decyzję o uznaniu PGE Toruń S.A. za Operatora Usługi Kluczowej w zakresie wytwarzania, dystrybucji i przesyłu ciepła, będziemy Państwa cyklicznie informować, na czym polegają zagrożenia cyberbezpieczeństwa w zakresie związanym ze świadczoną przez PGE Toruń S.A. usługą kluczową i o sposobach zabezpieczenia się przed nimi.**

Świat, w którym żyjemy otacza nas coraz szczelniej różnego rodzaju systemami komputerowymi i teleinformatycznymi, które ułatwiają nam zarówno załatwianie zawiłych spraw urzędowych jak i upraszczają nam chociażby robienie zakupów. Takie systemy są również wykorzystywane do świadczenia przez PGE Toruń S.A. usług kluczowych. Musimy jednak pamiętać, że korzystanie z jakiegokolwiek systemu informatycznego narażone jest na szereg zagrożeń, prób ataków (wirusy, robaki, trojany, phishing, programy szpiegujące itp.), których złożoność nieustannie rośnie. Dlatego PGE Toruń S.A. pragnie wspierać Państwa, jako użytkowników dostarczanych przez nas usług, w budowaniu świadomości i wiedzy w obszarze zagrożeń z obszaru cyberbezpieczeństwa oraz skutecznych sposobów zabezpieczania się przed tymi zagrożeniami.