Informacje

PGE Energia Ciepła produkuje i dostarcza ciepło dla dużych, polskich miast, wśród których znajdują się: Kraków, Gdańsk, Gdynia, Wrocław, Rzeszów, Lublin, Bydgoszcz i Kielce, spółka jest obecna także w Toruniu, Zielonej Górze, Gorzowie Wielkopolskim, Zgierzu i Siechnicach, gdzie jest również dystrybutorem ciepła do klientów końcowych.

***

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 Energia Ciepła S.A. za Operatora Usługi Kluczowej w zakresie wytwarzania energii elektrycznej i wytwarzania ciepła, będziemy Państwa cyklicznie informować, na czym polegają zagrożenia cyberbezpieczeństwa w zakresie związanym ze świadczoną przez PGE Energia Ciepła S.A. usługą kluczową i o sposobach zabezpieczenia się przed nimi.

24.07.2019

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 Energia Ciepła 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 Energia Ciepła 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.

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.

***

28.08.2019

Kolejna porcja informacji z cyklu zagrożeń z dziedziny cyberbezpieczeństwa dotyczy tzw. phishingu.

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.

***

30.09.2019

Kolejna porcja informacji z cyklu zagrożeń z dziedziny cyberbezpieczeństwa dotyczy haseł.

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.

***

5.11.2019

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 Energia Ciepła S.A. za Operatora Usługi Kluczowej w zakresie wytwarzania energii elektrycznej i wytwarzania ciepła, będziemy Państwa cyklicznie informować, na czym polegają zagrożenia cyberbezpieczeństwa w zakresie związanym ze świadczoną przez PGE Energia Ciepła S.A. usługą kluczową i o sposobach zabezpieczenia się przed nimi.

Kolejna porcja informacji z cyklu zagrożeń z dziedziny cyberbezpieczeństwa dotyczy niebezpiecznych załączników pocztowych.

Korespondencja elektroniczna jest obecnie jedną z najpopularniejszych form komunikacji. Codziennie otrzymujemy kilka a czasem nawet kilkadziesiąt e-mail zarówno prywatnych jak i służbowych. Wiadomości tą drogą przesyłają banki, instytucje, dostawcy usług, partnerzy biznesowi, klienci i niestety również cyberprzestępcy. Oczywiście żaden z nich nie podpisze się w ten sposób lecz będzie chciał podszyć się pod znanego nam nadawcę o czym pisaliśmy kiedyś w części dotyczącej phishingu. Bardzo często wysyłają oni wiadomości zawierające złośliwe oprogramowanie, które groźne jest nie tylko dla samego odbiorcy wiadomości. Mogą w sprzyjających warunkach sparaliżować całą organizację. Jak to się dzieje?

Hakerzy bardzo często podszywając się pod znane firmy czy instytucje przesyłają w mailach odpowiednio spreparowane załączniki zawierające złośliwe oprogramowanie tzw. *mallware*.

Otworzenie załącznika powoduje uruchomienie kodu, który - niekoniecznie natychmiast - zaczyna żyć na komputerze ofiary doprowadzając do wyłudzeń, kradzieży czy szyfrowania danych. Jednym z najgroźniejszych są oprogramowania z grupy *ransomware*, szyfrujące w celu wymuszenia okupu stacje nie tylko odbiorcy wiadomości, ale również dzięki zdolności do przenoszenia się na inne komputery w sieci także inne stanowiska pracy. W ten sposób może w bardzo krótkim czasie zostać sparaliżowana sporej wielkości organizacja.

Jak się bronić przed takim atakiem? Zabrzmi banalnie, ale nie otwierać podejrzanych wiadomości a w szczególności załączników w nich przesłanych. Niestety ten błąd popełniamy bardzo często!

Bądźmy ostrożni w przypadku dziwnych wiadomości, których nie spodziewaliśmy się, albo co do którym mamy wątpliwości czy nie otrzymaliśmy ich omyłkowo.

Poinformujmy o takim fakcie administratora swojej sieci lub dostawcę usługi pocztowej. Bardzo ważne jest by mieć na stacji oprogramowanie antywirusowe z najnowszymi sygnaturami oraz, co zalecamy, zaporę sieciową, która jako element ochronny wspomaga nas w skutecznym zabezpieczeniu swojego komputera. Będąc pracownikiem nie otwierać prywatnej poczty na służbowym komputerze – ryzykujemy wówczas bezpieczeństwem nie tylko swoim ale również naszego pracodawcy.