Zadania z przedmiotu: Przygotowanie stanowiska komputerowego

Tematy: Zagrożenia wynikające z dostępu do internetu.

I. Teoria

Podstawowym zagadnieniem będzie "**ograniczanie ryzyka**". Po zastosowaniu wszystkich punktów nie gwarantujemy pełnej ochrony, jednak zachęcamy was do skorzystania z nich. **Zagrożenie w internecie** jest wszechobecne. Szczególnie nasilone w kierunku kradzieży pieniędzy, jednak jeśli utrudnimy złodziejom dostęp do naszego komputera, przy odrobinie szczęścia przejdą do włamywania się do kogoś gorzej zabezpieczonego, pozostawiając nas w spokoju.

1. Antywirus, antyspyware oraz firewall

Brzmi dość prosto i naprawdę tak jest, jednak wciąż może dziwić liczba osób, które z takich programów nie korzystają. Każdy komputer z dostępem do internetu powinien korzystać z **antywirusa**, **oprogramowania antyspyware** oraz **firewall**. Szczególnie ważne jest utrzymywanie ich w aktualnych wersjach oraz regularne skanowanie komputera.

Dobrą wiadomością jest to, że dostęp do produktów dobrej jakości jest obecnie bardzo ułatwiony. Wszyscy ważniejsi producenci oprogramowania sprzedają swoje produkty w zestawach "**internet security suites**", a każde z nich zawiera przynajmniej te trzy najważniejsze rodzaje programów. Co więcej, można je ściągnąć i kupić bezpośrednio przez internet. Jednak jeśli planujecie to zrobić, proponujemy, aby była to pierwsza czynność jaką wykonacie po podłączeniu się do sieci.

2. Zabezpieczenia behawioralne

Nie wszystkie programy są takie same. Każdy może samemu dobrać sobie **program antywirusowy**, **oprogramowanie antyspyware** oraz **firewall** często bez wydawania pieniędzy, a mimo to będą spełniały one swoje funkcje. Warto jednak sprawdzić czy pochodzące od różnych firm oprogramowanie nie będzie się ze sobą "gryzło".

Oprócz podstawowych aplikacji, w ofercie wielu firm znajdują się też inne programy zabezpieczające, takie jak **behawioralne aplikacje zabezpieczające** wykorzystujące także tradycyjne sprawdzanie sygnatur wirusów.

Jako pierwsza linia obrony, sprawdzanie sygnatur jest niedoścignione. Chodzi o moment kiedy kod programu próbującego coś zmienić w naszym komputerze jest porównywany z bazą danych, znanych już szkodliwych aplikacji. Umożliwia to bardzo często usunięcie programu zanim zdąży on narobić w naszym OS-ie jakiekolwiek szkody.

Problem polega na tym, że wystarczą minimalne zmiany, aby wirus stał się niewykrywalny przez tradycyjne oprogramowanie. Programy wykorzystujące sygnatury wirusów oszczędzają czas i środki ponieważ eliminują znaczną większość złośliwych programów. Pozostaje jednak mały odsetek wirusów stworzonych w bardzo sprytny sposób. Tu właśnie przydaje się **behawioralne oprogramowanie zabezpieczające**. Najwyższej jakości pakiety posiadają obydwie te funkcje.

3. Usuń śmieci i próbki

Twój komputer może być dostarczony z masą darmowych triali, które po skończeniu się okresu próbnego zaczną nachalnie zachęcać do kupna pełnych wersji. Nie ma w tym nic niebezpiecznego, jednakże takie "pop-upy" mogą znieczulić użytkownika na przeróżne, irytujące komunikaty. Taką formę "reklamy" często przyjmują także wirusy niewykryte przez przestarzałe oprogramowanie zabezpieczające.

4. Aktualizuj swoje oprogramowanie

Brak utrzymywania "świeżości" swojego oprogramowania spowoduje, że Twój komputer będzie "dziurawy". Wiele programów wymaga **aktualizacji**. Producenci naprawiają w ten sposób błędy, które mogą wykorzystać

programiści od złośliwego oprogramowania. Popularne programy takie jak Adobe Flash czy Firefox, jak również system operacyjny Windows, wymagają regularnych aktualizacji, ponieważ ich brak skutecznie obniża **poziom bezpieczeństwa**.

Tam gdzie to tylko możliwe zalecamy zaznaczenie funkcji **automatycznej aktualizacji**. Jeśli nie wiecie jak tego dokonać to skorzystajcie z programów typu **Secunia PSI**, które zaktualizują je za was.

5. Załóż konto do kontroli wszystkich kont

Jednym z najłatwiejszych sposobów poprawienia bezpieczeństwa jest korzystanie z konta o ograniczonych możliwościach tak, aby nie było możliwe dokonanie żadnych krytycznych zmian w systemie. Aby to zrobić, na początku należy stworzyć **konto administratora** i ustawić aby tylko ono było wstanie dokonywać ważnych zmian. Następnie założyć chronione hasłem **konto o ograniczonych możliwościach**, które będzie wykorzystywane na co dzień.

Pomaga to zapobiegać bezpośrednim interwencjom w komputer, które mogą doprowadzić do poważnych szkód, o których wspomnimy niżej.

6. Zabezpiecz sieć oraz przeglądarkę

Istnieje kilka rzeczy jakie możesz zrobić w celu zabezpieczenia komputera przez zagrożeniami płynącymi z sieci. Pierwsza to zabezpieczenie swojego routera. Mimo iż standardowo posiada on hasło, to często brzmi ono "1234" lub "0000". Ustawmy więc jakieś bardziej skomplikowane, najlepiej szyfrowane w **standardzie WPA2**. W samej przeglądarce, zabezpieczenia mogą zostać ustawione na te najbardziej restrykcyjne.

7. Ustaw punkt przywracania systemu

Punkt przywracania systemu jest swego rodzaju zakładką, która jest tworzona po znaczącej zmianie w twoim komputerze. **Windows Updates** tworzy je po instalacji większych aktualizacji. Często **punkt przywracania** tworzony jest również w określonych odstępach czasowych np. co tydzień. Jeśli czasem pójdzie coś źle i np. wprowadzone zostaną bardzo niekorzystne ustawienia, punkty te umożliwią powrót do poprzedniego momentu, bez straty wielu ważnych danych.

8. Uświadom innych użytkowników komputera

Podstawowym i największym zagrożeniem dla komputera jest jego użytkownik. Najłatwiejszym natomiast sposobem na zainfekowanie sprzętu wirusem jest dopuszczenie nieświadomego użytkownika, który wejdzie w nieodpowiedni link lub ściągnie plik niewiadomego pochodzenia.

Element ludzki nigdy nie zostanie całkowicie wyeliminowany, jednakże można ograniczyć niebezpieczeństwo uzgadniając klika podstawowych zasad dotyczących użytkowania Twojego nowego komputera. Powinni ich przestrzegać wszyscy, również Ty.

Strony, które uważasz za nieodpowiednie można bezproblemowo dodać do czarnej listy przy pomocy darmowych programów takich jak **Windows Family Safety**. Zatrzymaj prawa administratora tylko dla siebie. Zaznacz, że ściąganie plików niewiadomego pochodzenia nie będzie tolerowane, hasła powinny być zróżnicowane i nie banalne.

9. Fizyczne zabezpieczenie

Laptopy mają jeden poważny minus: łatwo je ukraść. Powinniśmy zastosować się do dwóch prostych zasad, aby temu zapobiec. Jeśli to możliwe trzymać sprzęt blisko łóżka w którym śpimy i koniecznie przechowywać go w miejscu odległym od okien i niewidocznym z ulicy. Kolejnym sposobem może być inwestycja w **zabezpieczenie Kensingston** i fizyczne przyczepienie komputera do czegoś. Nikt z pewnością nie chciałby się zorientować, że jego idealnie zabezpieczony komputer został fizycznie ukradziony.

10. Bądź uważny i rozważny

Żadna z powyższych rad nie zagwarantuje bezpieczeństwa waszemu systemowi. Jednak zestawione razem spowodują, że ewentualny cyberprzestępca będzie miał dużo bardziej ograniczony dostęp do waszego komputera, a w najgorszym przypadku do waszego portfela. Kluczem do tego wszystkiego jest zachowanie czujności.

II.Pojęcia:

Dostępność - system i informacje mogą być osiągalne przez uprawnionego użytkownika w każdym czasie i w wymagany przez niego sposób

Poufność - informacje ujawniane są wyłącznie uprawnionym podmiotom i na potrzeby określonych procedur, w dozwolonych przypadkach i w dozwolony sposób

Prywatność - prawo jednostki do decydowania o tym, w jakim stopniu będzie się dzielić z innymi swymi myślami, uczuciami i faktami ze swojego życia osobistego

Integralność - cecha danych i informacji oznaczająca ich dokładność i kompletność oraz utrzymanie ich w tym stanie

Uwierzytelnianie osób – zagwarantowanie, że osoba korzystająca z systemu jest rzeczywiście tą, za którą się podaje

Uwierzytelnianie informacji – zagwarantowanie, że informacja rzeczywiście pochodzi ze źródła, które jest w niej wymienione

Niezaprzeczalność – brak możliwości zaprzeczenia faktowi wysłania lub odebrania informacji

Zadanie:

1.Napisz jak zabezpieczyć nasz komputer oraz oprogramowanie w swoim komputerze?

2. Rozwiń dwa dowolne pojęcia z punktu **II.Pojęcia**

Zadanie proszę odesłać w formie elektronicznej: pdf, doc, lub odt na adres poczty służbowej w.stankiewicz@ckziu-elektryk.pl.

klasa_nazwisko_imie_przedmiot_numer_zadania_kolejny_numer_pliku. rozszerzenie

np.

1ctz_nowak_jan_przygotowanie_stanowiska_komputerowego_zad01_01.doc

lub

spakować wszystkie pliki zachowując strukturę nazewnictwa jak wyżej z rozszerzeniem np. zip

Zwracam uwagę przy ocenianiu na dokument który państwo mi wysyłają tzn. strona tytułowa, spis treści, zastosowana czcionka, formatowanie dokumentu, bibliografia i czytelność opisu itd.

Termin oddania: 27.03.2020r.