Cyber MSME

Cyberbezpieczeństwo dla mikro, małych i średnich firm

Cyberbezpieczeństwo przy ograniczonym budżecie

Jak chronić swoją firmę, gdy liczy się każdy grosz?

Autorzy: CTS Customized Training Solutions i CASE

Erasmus+

Wsparcie Komisji Europejskiej dla powstania tej publikacji nie oznacza poparcia dla jej treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

Zanim zaczniemy...

Przedstawiony tu zestaw narzędzi najlepiej nadaje się dla mikro i małych firm (a także do użytku osobistego), które chcą wzmocnić swoje bezpieczeństwo cybernetyczne przy niewielkim budżecie. Zarekomendujemy Ci konkretne oprogramowanie i sprzęt, wskażemy Ci też odpowiednie narzędzia. Zachęcamy Cię oczywiście do tego, abyś sam/-a także przeszukał/-a sieć pod tym kątem.

Wstęp

Kiedy mówimy o cyberbezpieczeństwie, hakerstwie, serwerach i tym podobnych, myślimy o tych rzeczach w sposób, jaki wpoiły nam filmy z Hollywood. Wyobrażamy sobie futurystyczną technologię, firmy warte wiele miliardów dolarów, hakerów skrytych w mroku, szybko piszących na klawiaturze, wielkie serwerownie i interfejsy tekstowe (to ostatnie jest w zasadzie prawdą). To prowadzi nas do myślenia, że wszystkie te rzeczy są zarezerwowane dla wielkich organizacji z milionowymi funduszami na ich wsparcie. Ale czy można wdrożyć narzędzia cyberbezpieczeństwa w małym i średnim przedsiębiorstwie, pracującym z ograniczonym budżetem? Oczywiście! Pokażemy Ci, jak to zrobić.

Wsparcie Komisji Europejskiej dla powstania tej publikacji nie oznacza poparcia dla jej treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

Rozwiązania zewnętrzne a rozwiązania własne

Zanim zaczniemy mówić o VPN-ach i ad-blockerach wyjaśnijmy słownictwo, którym będziemy się posługiwać polecając pewne rozwiązania.

Rozwiązanie zewnętrze

Oznacza to, że ktoś (inna firma) wykona pracę za Ciebie. Zazwyczaj wszystko, co Ty musisz zrobić, to instalacja aplikacji lub inne podstawowe czynności – konfiguracją i hostingiem zajmuje się firma zewnętrzna.

Plusy:

Łatwość konfiguracji i dostępu; nie są wymagane dodatkowe umiejętności i wiedza; wysoce konkurencyjny rynek sprawia, że różne firmy oferują wiele dodatkowych usług.

Erasmus+

W sparcie Komisji Europejskiej dla powstania tej publikacji nie oznacza poparcia dla jej treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

Minusy:

Plany płatności mogą nie być dostosowane do Twoich potrzeb, co sprawia, że płacisz za rzeczy, których nie potrzebujesz lub nie używasz; powierzasz swoje dane zewnętrznej firmie; ceny subskrypcji szybko sumują się w duże kwoty.

Self-hosting:

Oznacza, że to Ty jesteś odpowiedzialny za hosting swoich narzędzi cyberbezpieczeństwa. Oprócz urządzenia, na którym będziesz je hostował, potrzebujesz również odpowiedniego oprogramowania oraz wiedzy, aby je poprawnie zainstalować i skonfigurować.

Plusy:

Dostajesz dokładnie to, czego chcesz; uczenie się nowych rzeczy może być zabawne i pełne wyzwań; masz szeroki wybór oprogramowania open-source dostępnego za darmo z wielkim wsparciem społeczności; możesz poczuć się jak filmowy haker nagle używając Linuksa i linii poleceń :)

Erasmus+

Wsparcie Komisji Europejskiej dla powstania tej publikacji nie oznacza poparcia dla jej treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

Minusy:

Wymagana podstawowa/średnia znajomość komputera; potrzebny serwer, który jest kosztem samym w sobie.

Samodzielny hosting przy niskim budżecie

Kończąc czytać o self-hostingu, prawdopodobnie zadałeś sobie pytanie "Kto by wybrał taką opcję? Nie wiem nic o serwerach i nie chcę wydawać tysięcy na infrastrukturę!". Rzecz w tym, że nie musisz wydawać tysięcy złotych na infrastrukturę. Prawdę mówiąc, nie musisz jej nawet posiadać!

Przede wszystkim, cloud hosting jest powszechnie dostępny. Wszyscy wielcy gracze świata IT (Amazon, Google, Microsoft) oferują platformy w chmurze, a to nie wszystko – istnieją dziesiątki i są oferowane przez mniejsze firmy (np. DigitalOcean i Heroku). Wszystkie z nich oferują bezpłatny okres próbny (1 do 3 miesięcy w zależności od platformy), więc masz czas, aby je sprawdzić i spróbować self-hostingu bez konieczności opłaty z góry.

Erasmus+

Wsparcie Komisji Europejskiej dla powstania tej publikacji nie oznacza poparcia dla jej treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

Po zakończeniu darmowego okresu próbnego, opłaty za maszynę wirtualną zdolną do hostowania oprogramowania wymienionego w tym zestawie narzędzi wyniosłyby około 5-10 euro miesięcznie, co prawdopodobnie wyniesie mniej niż subskrypcje innych firm łącznie.

A co z posiadaniem własnego serwera? Nie byłoby to opłacalne i nie zajmowałoby dużo miejsca, prawda?

Wręcz przeciwnie! Urządzenie odpowiednie dla Twojego MŚP może kosztować Cię mniej niż 100 euro i mieścić się w dłoni. Poznaj Raspberry PI, mały, wszechstronny komputer:

Nasze Rapsberry PI z mandarynką dla skali. Mandarynka była pyszna.

Erasmus+

Wsparcie Komisji Europejskiej dla powstania tej publikacji nie oznacza poparcia dla jej treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

Oprócz tego, że może być VPNem i ad-blockerem (jednocześnie!), można go wykorzystać do dziesiątków różnych rzeczy (serwery multimedialne, dysk sieciowy, automaty do gier, inteligentne lustra, emulatory konsol retro – możliwości są ogromne). Najnowsze modele mogą być również wygodnie wykorzystywane jako zapasowy komputer PC w przypadku nagłej awarii. Przy cenie oscylującej wokół 60-100 euro w zależności od modelu, może to być najbardziej opłacalne rozwiązanie na dłuższą metę.

VPN

Co to jest VPN i dlaczego warto z niego korzystać, wyjaśniliśmy już szczegółowo w naszych innych materiałach (które gorąco polecamy!), ale w ramach przypomnienia: VPN to wirtualna sieć, która chroni Waszą prywatność poprzez ukrywanie przesyłanych danych w dodatkowej warstwie szyfrowania. Jest on używany przede wszystkim jako warstwa ochrony w czasie korzystania z publicznych lub niezabezpieczonych sieci, by źli aktorzy nie mogli zdobyć Twoich danych. W wiele firm oferuje usługi VPN i intensywnie je reklamuje (jeśli jesteś częstym użytkownikiem/ użytkowniczką YouTube'a, to na pewno widziałeś/-aś co najmniej jedną reklamą VPNa).

Erasmus+

W sparcie Komisji Europejskiej dla powstania tej publikacji nie oznacza poparcia dla jej treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

Warte uwagi opcje VPN:

Zewnętrzne:

Nie będziemy wymieniać konkretnych, ponieważ rynek jest bardzo konkurencyjny, a różnice między najlepszymi dostawcami są minimalne. Wpisanie hasła "najlepszy VPN + aktualny rok" pozwoli Ci uzyskać wyniki w kilka sekund.

Ceny: około 10euro/miesiąc w planie miesięcznym (porównując oferty czołowych dostawców), taniej przy zakupie w planach długoterminowych (3-5 euro miesięcznie).

Self-hosted:

OpenVPN (https://openvpn.net/vpn-software-packages/) **Ceny:** Open source/ bezpłatny

AlgoVPN (https://github.com/trailofbits/algo) **Ceny:** Open source/ bezpłatny

Erasmus+

Wsparcie Komisji Europejskiej dla powstania tej publikacji nie oznacza poparcia dla jej treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

Ad-blockery

Do tego czasu już zapewne słyszałeś/-aś o ad-blockerach. Istnieje nawet duże prawdopodobieństwo, że używasz jakiegoś teraz (i słusznie)! Ad-blockery to długo poszukiwana odpowiedź na natrętne, pełnostronicowe reklamy, które nękały użytkowników Internetu. Umożliwiają one bardziej przyjazne

Dla użytkownika podejście do reklam w sieci, ale mogą również znacznie zwiększyć bezpieczeństwo w Twojej firmie. W jaki sposób?

Wprowadzające w błąd lub złośliwe reklamy są jednym z głównych sposobów, w jaki można narazić

bezpieczeństwo małej firmy. Użytkownik albo klika na taką reklamę przez pomyłkę, albo zostaje zwabiony obietnicą darmowego tabletu, który ot tak po prostu wygrał. Ponadto wszystkie reklamy zużywają limit danych Twojego Internetu, co może być ważnym czynnikiem, gdy znajdujesz się w miejscu z ograniczonym dostępem do sieci lub używasz danych pakietowych. Gdyby Twój food truck był w drodze, to zapewne wolałbyś/ wolałabyś zużywać cenny limit danych internetowych do sprawdzania portalu z dostawawami, a nie reklamy pigułki-cud. Jakie zatem są Twoje opcje?

Erasmus+

W sparcie Komisji Europejskiej dla powstania tej publikacji nie oznacza poparcia dla jej treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

Porozmawiajmy jeszcze o dwóch rodzajach ad-blockerów. Pierwszym z nich jest ad-blocker po stronie klienta, który instalujesz w swojej przeglądarce. Drugi to ad-blocker oparty na rozwiązywaniu DNS. Blokery po stronie klienta są instalowane jako dodatek do przeglądarki. Serwery DNS wymagają maszyny, na której będą działać. Jaka jest różnica?

Wyobraź sobie film ze sceną dla dorosłych, której nie chcesz oglądać. Blokery po stronie klienta byłyby jak zakrycie oczu rękami. Nie mogłeś tego zobaczyć, ale to wciąż tam było. Film trwał dłużej, a Twój rachunek za prąd był z tego powodu wyższy. Można by pomyśleć, że koszty nie byłyby wysokie przez kilka sekund, ale wyobraź sobie, że zakrywasz oczy setki razy każdego dnia! Koszt w końcu by się podniósł. Serwer DNS wyciąłby dla Ciebie scenę z programu TV jeszcze przed jego emisją, dzięki czemu film byłby krótszy, a utrzymanie rachunku za energię elektryczną – niższe. Inną ważną zaletą jest to, że można użyć serweru DNS na poziomie sieci, dzięki czemu urządzenie, łącząc się z siecią, jest chronione przed reklamami. Nie musisz wtedy instalować klienta blokera dla każdej przeglądarki na każdym używanym w firmie komputerze.

Wsparcie Komisji Europejskiej dla powstania tej publikacji nie oznacza poparcia dla jej treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

Godne uwagi opcje blokowania reklam przy pomocy DNS:

Zewnętrzne:

NextDNS (https://nextdns.io) - darmowy plan osobisty ograniczony do 300k żądań miesięcznie, plan Pro to około 2 euro miesięcznie, plan biznesowy zaczynający się od około 200 euro rocznie do 50 **pracowników.**

Ceny: około 10euro/miesiąc na planie miesięcznym (porównując oferty czołowych dostawców), taniej przy zakupie w planach długoterminowych (3-5 euro miesięcznie).

Self-hosted:

Pi-hole (https://pi-hole.net) - instrukcja montażu znajduje się na stronie: https://github.com/pi-hole/

Cena: open source/bezpłatny

Erasmus+

W sparcie Komisji Europejskiej dla powstania tej publikacji nie oznacza poparcia dla jej treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

Dziękujemy za uwagę!

Wsparcie Komisji Europejskiej dla powstania tej publikacji nie oznacza poparcia dla jej treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.