Cyber MSME

Cyberbezpieczeństwo dla mikro, małych i średnich f irm

Kluczowe zasady zabezpieczeń routera

Zwiększ bezpieczeństwo swojej sieci dzięki kilku podstawowym krokom

Autorzy: CTS Customized Training Solutions i CASE

Erasmus+

Stosując się do tych prostych wskazówek, możesz sprawić, że sieć Twojej małej firmy będzie znacznie bezpieczniejsza:

1. Sprawdź datę produkcji routera

Twój zaufany router jest z Tobą od początku istnienia firmy? Czy traktujesz go jak honorowego pracownika? Rozumiemy to, naprawdę! Ale kiedy stawką jest bezpieczeństwo Twojej firmy, nie ma miejsca na sentymenty.

Nie ma prostego sposobu, aby ustalić, czy powinieneś/ powinnaś zmienić swoje urządzenie, czy nie. Eksperci zalecają wymianę routera co 2-3 lata, a absolutne maksimum to 5 lat. Należy natychmiast zmienić urządzenie, jeśli obsługuje ono tylko protokół szyfrowania, o którym wiadomo, że ma poważne luki w zabezpieczeniach (więcej informacji na ten temat pojawi się później).

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

2. Zaktualizuj oprogramowanie sprzętowe

Kupujesz nowy router, konfigurujesz podstawy, a nigdy więcej nie dotykasz panelu administracyjnego? Wszyscy tak robiliśmy! Ale jest dobry powód, aby zajrzeć do panelu od czasu do czasu. Routery, jak każde inne urządzenie podłączone do Internetu, otrzymują ciągłe aktualizacje oprogramowania.

Podczas gdy niektóre urządzenia aktualizują się automatycznie, niektóre wymagają do tego ingerencji administratora — jeśli po prostu zostawisz to tak jak jest, możesz przegapić ważne aktualizacje zabezpieczeń, a to może zostać wykorzystane przez złych aktorów do uzyskania dostępu do Twojej sieci!

3. Włącz funkcję Wi-Fi Protected Setup (WPS)

Podczas wizyty w panelu administracyjnym należy pamiętać o wyłączeniu funkcji WPS. Co to jest WPS? Jest to metoda podłączania nowego urządzenia do sieci poprzez wciśnięcie fizycznego przycisku na routerze. Może wydawać się to wygodne (nie musisz zapamiętywać hasła!), ale jest to naprawdę niebezpieczne. Dlaczego?

Erasmus+

WPS to najczęstszy sposób uzyskiwania przez hakerów **nieautoryzowanego dostępu do sieci**.

Wiele narzędzi hakerskich wykorzystuje WPS wyłącznie jako metodę naruszenia bezpieczeństwa sieci. **Wyłączenie tej funkcji to jeden z najprostszych i najważniejszych kroków do zapewnienia bezpieczeństwa sieci!**

4. Nie używaj protokołów szyfrowania WEP lub WPA (chyba że musisz)

Podczas konfigurowania sieci Wi-Fi pojawią się pytania, czy chcesz, aby Twoja sieć była chroniona hasłem (chcesz), a jeśli tak, to jakiego protokołu szyfrowania chcesz użyć. W tym miejscu większość

z nas zaczyna panikować, ponieważ jesteśmy bombardowani enigmatycznymi skrótami (WEP, WPA, WPA-PSK, WPA2-PSK i wiele innych). Dlaczego jest ich tak dużo? Który z nich wybrać? Pozwól nam odpowiedzieć na te pytania.

W uproszczeniu: protokoły szyfrowania są sposobem na autoryzację tylko tych połączeń, które posiadają wymagany klucz (w naszym przypadku hasło do Wi-Fi) i trzymają innych z dala. WEP był pierwszym ratyfikowanym standardem, a jego początki sięgają 1999 roku. W 2003 roku został on

Erasmus+

zastąpiony przez WPA (Wi-Fi Protected Access), po którym w 2004 roku pojawił się WPA2. Od 2018 roku dostępny jest WPA3.

Więc który z nich powinieneś użyć? Prosta odpowiedź: najnowszy, jaki obsługuje Twój router. Jeśli router pozwala tylko na korzystanie z szyfrowania WEP lub WPA, rozważ wymianę urządzenia tak szybko, jak to możliwe. Oba te protokoły mają znane luki, które umożliwiają hakerom uzyskanie dostępu do sieci w ciągu zaledwie kilku minut za pomocą publicznie dostępnych narzędzi. WPA2 jest obecnie najbardziej powszechne, ale jeśli planujesz zmienić router w najbliższej przyszłości, kup urządzenie, które obsługuje Wi-Fi 6 i WPA3.

Dlaczego więc te "niebezpieczne" wciąż są w pobliżu? Należy pamiętać, że urządzenie łączące się z routerem również musi być w stanie korzystać z protokołu szyfrowania. Nierzadko zdarza się, że firma korzysta z konkretnego urządzenia, które może działać tylko na starszym protokole.

W takim przypadku należy rozważyć utworzenie dodatkowej sieci dla tego urządzenia, aby uniknąć narażania wszystkich urządzeń.

Erasmus+

5. Utwórz oddzielną sieć dla gości

"Czy mogę skorzystać z Twojego Wi-Fi?" — to pytanie, które prędzej czy później usłyszysz, prowadząc firmę. Choć w 95% przypadków jest to zrozumiała (i zupełnie niewinna) prośba, ostrożności nigdy nie dość, zwłaszcza w kwestiach bezpieczeństwa. Zwróć uwagę, że większość nowoczesnych urządzeń pozwala na utworzenie sieci dla gości za pomocą kilku naciśnięć przycisku. Pamiętaj: choć Twoi goście mogą mieć najlepsze intencje, ich urządzenia mogą być zainfekowane bez ich wiedzy.

6. Przede wszystkim: używaj hasła do ochrony sieci ☺

Oczywiście wszystkie wcześniejsze wskazówki są ważne, ale ta jest kluczowa. Wcześniejsze kroki nie zadziałają, jeśli nie zaczniesz od hasła ☺ (o bezpiecznych hasłach dowiesz się więcej z naszego opracowania "Ulepsz swój plan zarządzania cyberbezpieczeństwem - dobre praktyki").

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Dziękujemy za uwagę!

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained