CyberMSME

Cyberbezpieczeństwo dla mikro, małych i średnich firm

Ulepsz swój plan zarządzania cyberbezpieczeństwem - dobre praktyki

Autorzy: CTS Customized Training Solutions i CASE

Erasmus+

Spis treści — kliknij, aby przejść do odpowiedniej strony:

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.

Możesz ulepszyć swój plan zarządzania cyberbezpieczeństwem, postępując według poniższych wskazówek:

1. Wzmocnij hasła

Wydaje się oczywiste, że silne hasło jest pierwszą linią obrony przed włamaniami. Zmienianie haseł zbyt rzadko ułatwia hakerom ich złamanie.

Hasła — dobre praktyki

Być może słyszałeś, że najlepsze hasło zawiera co najmniej 1 dużą literę, co najmniej 1 cyfrę i co najmniej 1 symbol (jak % # &). Musi mieć więcej niż 7 znaków. Zerknij na przykład na kolejnej stronie.

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.

Powiedzmy, że Twój pies ma na imię Rysio. Zaadoptowałeś/-aś go w 2018 roku. Zatem hasło na Twoim laptopie, służbowej chmurze i służbowej poczcie elektronicznej to Rysio-2018. Łatwe do zapamiętania, prawda?

Niestety jest także łatwe do złamania.

Co możesz zrobić?

Dowiedz się, jak tworzyć silne hasła. Dobre, trudne do złamania hasło musi być:

- **długi (nie krótszy niż 15 znaków)**
- **mieszanka małych i dużych znaków**
- **nie zawiera typowych substytutów (np. "h0m3" zamiast "home" jest zbyt oczywiste)**
- **nie zawiera typowych ścieżek klawiaturowych (jak "qwerty", "12345")**

Erasmus+

Używaj managera haseł

Menedżer haseł to program komputerowy, usługa internetowa lub wtyczka, która umożliwia użytkownikom generowanie i zarządzanie hasłami. Polecamy Twojej uwadze Keeper, LastPass lub DashLane.

Jeśli jednak nie możesz się zdecydować, to pod tym linkiem przeczytasz więcej o różnych menedżerach haseł i ich specyfikacjach:
https://en.wikipedia.org/wiki/List_of_password_managers

2. Zamiast haseł zastosuj frazy dostępu (passphrase)

Fraza dostępu (passphrase) to kombinacja słów i symboli, które tworzą zdanie. Zdanie to nie musi być poprawne gramatycznie. Frazy dostępu zawierają zazwyczaj do 40 znaków. W odróżnieniu od haseł frazy dostępu zawierają spacje.

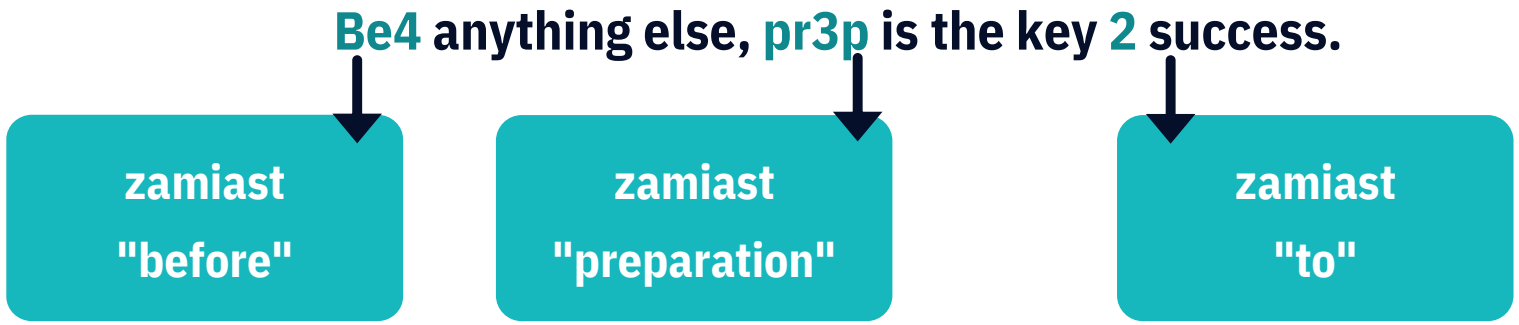
Erasmus+

Frazy dostępu — dobre praktyki

- Użyj łatwej do zapamiętania, ale niecodziennej frazy.
- Użyj niecodziennych i/lub skróconych słów.
- Dodaj spacje.
- Użyj dużych liter (na początku zdania lub dla wybranych słów).
- Zamień niektóre litery na cyfry.
- Dodaj interpunkcję.

Polecane linki: TechTarget > Passphrase (https://searchsecurity.techtarget.com/definition/passphrase);
John Carroll University > Password vs Passphrase (https://password.jcu.edu/public/passphrase.php)

Fraza dostępu może wyglądać jak słowa Aleksandra Grahama Bella:



Albo jak przypadkowe słowa i cyfry:

SaMieC p13s 21, mi3jscE n4 P0dium.

Na cokolwiek się zdecydujesz, pamiętaj o regularnej zmianie haseł. Nie zapisuj ich tam, gdzie ktoś inny mógłby uzyskać do nich dostęp. Zdecyduj, kto powinien je znać — przecież nie każdy w Twoim zespole musi znać każde hasło i frazę.

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.

3. Tam, gdzie to możliwe, stosuj więcej niż 1 warstwę uwierzytelniania

Haker może złamać nawet silne hasło lub frazę dostępu. Dlatego jeśli tylko możesz, używaj uwierzytelniania dwuskładnikowego (2FA). 2FA to dodatkowa warstwa zabezpieczająca dla Twojego hasła lub frazy dostępu stworzona po to, aby zagwarantować, że nikt poza Tobą zaloguje się na Twoje konto, nawet jeśli zna hasło.

Jak działa 2FA?

- 2FA można znaleźć w wielu aplikacjach i serwisach internetowych. W pierwszym kroku używasz swojego loginu i hasła/ frazy dostępu – jak zwykle.
- W kolejnym kroku aplikacja/ serwis internetowy wysyła Ci tymczasowy kod weryfikacyjny (np. na Twój numer telefonu komórkowego). Kod ten należy wpisać w aplikacji/ serwisie internetowym, aby się zalogować.
- Inną możliwością 2FA jest biometryczny skan odcisku palca lub twarzy.

Erasmus+

4. Nigdy nie wysyłaj nikomu swojego hasła SMS-em ani e-mailem

W przypadku konieczności udostępnienia pracownikom niektórych haseł lub fraz dostępu, użyj menedżera haseł, takiego jak Keeper, LastPass lub DashLane.

5. Wybieraj trudne do odgadnięcia pytania zabezpieczające

Podczas tworzenia konta często trzeba wybrać pytanie zabezpieczające na wypadek, gdybyś zapomniał/-a hasła. Na większość z tworzonych pytań można jednak łatwo znaleźć odpowiedzi na Twoich kanałach social media (np. Twój ulubiony film, data pierwszej randki, imię pierwszego kota, itp.)

Bądź tego świadomy/-a i starannie dobieraj pytania. Naucz tego także swoich pracowników i partnerów.

Polecany link: Avast > How to create a strong password (https://blog.avast.com/strong-password-ideas)

Erasmus+

6. Regularnie aktualizuj wszystkie aplikacje

Upewnij się, że Twoje oprogramowanie antywirusowe jest regularnie aktualizowane. Skanuj swój komputer przynajmniej raz w tygodniu. Pamiętaj, że każde połączenie z Internetem to okoliczność sprzyjająca atakom, a prawdopodobnie używasz Internetu codziennie przez wiele godzin.

Dbaj również o aktualizacje systemu operacyjnego, przeglądarki internetowej, chmury, aplikacji do komunikacji itp. Najmniejsza luka w zabezpieczeniach może ułatwić hakerom atak na Twoją firmę.

7. Regularnie aktualizuj swoje urządzenia

Przedsiębiorcy często zapominają o aktualizowaniu urządzeń innych niż laptopy czy smartfony. Jednak wszystkie firmy posiadają więcej rzeczy, które mogą stać się celem hakerów. Sprawca może włamać się do Twojego routera, drukarki lub faksu. Upewnij się, że firmware jest aktualny we wszystkich urządzeniach posiadających połączenie wifi — nawet w mikrofalówce i piekarniku w kuchni.

Erasmus+

8. Zachowaj ostrożność podczas korzystania z publicznego wifi

Publiczne wifi jest dostępne niemal wszędzie, z punktami dostępu gotowymi do korzystania w restauracjach, kawiarniach czy na lotniskach. Jako przedsiębiorca/ przedsiębiorczyni możesz potrzebować dostępu do Internetu w różnych miejscach. Pytanie brzmi: czy jesteś bezpieczny/-a korzystając z publicznego WiFi?

Jeśli tylko jest to możliwe, staraj się korzystać z Internetu od swojego dostawcy. Możesz zrobić ze swojego telefonu hotspot lub kupić dedykowane temu urządzenie. Jest to dużo bezpieczniejsze niż publiczne wifi, które ze względu na ogólną dostępność może być podatne na ataki hakerów czyhających na poufne dane.

Co może ochronić Ciebie i Twój biznes, kiedy korzystasz z publicznego wifi?

Najlepszą i najbardziej dostępną opcją jest skorzystanie z VPNa w celu ochrony swojej prywatności.

Polecany link: Kaspersky > **Public Wifi Security** (https://www.kaspersky.com/resource-center/preemptive-safety/public-wifi)

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.

Czym jest VPN?

VPN to skrót od Virtual Private Network (wirtualna sieć prywatna). "Wirtualna" oznacza, że sieć nie istnieje w rzeczywistości w sposób fizyczny, ale jest tworzona przez oprogramowanie. "Prywatna" tłumaczy się sama: jest to sieć, do której nie można swobodnie dotrzeć w Internecie. Jest ona zazwyczaj znacznie bezpieczniejsza niż sieć publiczna, ponieważ ogranicza połączenia, a dane nie mogą być łatwo szpiegowane przez hakerów czyhających w sieci publicznej.

Jak uzyskać dostęp do VPNa?

Możesz skonfigurować własną sieć VPN lub skorzystać z jednego z wielu płatnych dostawców usług VPN. Bądź ostrożny/-a! Choć możesz natknąć się na darmowe VPNy w sieci, korzystanie z nich może być jednak bardziej niebezpieczne niż korzystanie z darmowego wifi na lotnisku. Wszystko wynika z tego, jak działają VPN-y.

Polecany link: Algo VPN > **Self hosted VPN solution** (https://github.com/trailofbits/algo)

Erasmus+

Jak działa VPN?

Kiedy uzyskujesz dostęp do dowolnego zasobu w Internecie, cała komunikacja odbywa się za pośrednictwem pakietów. Mówiąc prościej, pakiet to mała porcja danych, która przechodzi przez różne trasy, aby dotrzeć do miejsca docelowego. Oto jak wygląda uproszczone "życie" pakietu bez VPN.

Zauważ jak twoje pakiety podróżują niezaszyfrowane przez darmową sieć wifi. Każdy haker, który uzyskał dostęp do darmowej sieci wifi może przechwycić, a tym samym wykraść wszelkie wrażliwe dane, które wysyłasz/ odbierasz.

Teraz porównajmy to z "życiem" pakietu z włączonym VPNem:

Jak widać, pakiet jest szyfrowany na całej drodze do serwera VPN. Jak to się dzieje? Klient VPN zainstalowany na Twoim urządzeniu zamyka oryginalny pakiet w inny, zaszyfrowany. Ten zaszyfrowany pakiet jest następnie przesyłany przez darmową sieć wifi i dostawcę usług internetowych do serwera VPN. Wreszcie, serwer VPN odszyfrowuje oryginalny pakiet i przekazuje go do oryginalnego miejsca docelowego.

Porównując to z poprzednim przykładem, nawet jeśli hakerzy będą mieli dostęp do zaszyfrowanych pakietów w wolnej sieci, nadal będą musieli złamać szyfrowanie, aby zobaczyć Twoje dane.

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.

Wady wynikające z używania VPNa

Oczywiście istnieją wady wynikające z używania sieci VPN. Przede wszystkim VPN, którego użyjesz, musi być całkowicie godny zaufania. Gdy korzystasz z sieci publicznej, ktoś może próbować przechwycić Twoje dane. Gdy korzystasz z VPNa, to z założenia przechwyci on wszystkie Twoje dane. Oznacza to, że VPNy skonfigurowane tak, aby szkodzić, są niezwykle niebezpieczne dla Twojej firmy.

Ponadto popularni dostawcy VPNów, jako że zapewniają bezpieczeństwo, to przyciągają często użytkowników będących tzw. złymi aktorami. Może się nagle okazać, że zostaniesz pozbawiony dostępu do popularnych stron lub zasobów, bo dzielisz ten sam końcowy adres IP z kimś, kto używał go w złym celu w przeszłości.

Wreszcie — prędkość. Dodatkowa warstwa ochrony zazwyczaj ogranicza prędkość, z jaką można uzyskać dostęp do zasobów. Podczas gdy jest to nieistotne w trakcie korzystania z darmowych sieci wifi (poczynając od tego, prędkość Internetu w takich sieciach nie jest bardzo wysoka), to w przypadku sieci domowej może ograniczyć jej wydajność.

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.

9. Stwórz spis swoich zasobów

W dzisiejszych czasach prowadzenie własnej firmy wymaga od Ciebie i Twoich pracowników znacznie więcej niż jeszcze kilka lat temu. Musisz zapamiętać wiele nazw aplikacji, loginów, haseł itp. Co by było, gdyby ktoś zapomniał swoich danych uwierzytelniających? Co jeśli jeden z Twoich pracowników zgubiłby swój smartfon? Co powinieneś/ powinnaś wtedy zrobić?

Przede wszystkim przygotuj swoją firmę na wszelkie możliwości, tworząc spis swoich zasobów. Taki spis musi zawierać wszystkie dane o urządzeniach i usługach online.

Ty lub Twój ekspert ds. cyberbezpieczeństwa powinniście przygotować spis zasobów i regularnie go aktualizować. W przypadku jakiegokolwiek ataku, zawsze będziesz mieć wszystkie dane niezbędne do wdrożenia planu zarządzania cyberkryzysem.

Jak przygotować spis zasobów firmowych?

Erasmus+

Przykładowy spis zasobów

- **Lista urządzeń** > model, pamięć, pojemność dysku, system operacyjny, IP, numer seryjny > aktualny użytkownik (imię i nazwisko pracownika) > data spisu
- **Ustawienia konfiguracji w celu określenia, czy urządzenie jest bezpiecznie skonfigurowane** > specyfikacja, data aktualizacji> data spisu
- **Połączenia sieciowe, zabezpieczenia sieciowe i VPN** > dostawca, lokalizacja, status, konfiguracja > data spisu
- **Oprogramowanie antywirusowe i inne oprogramowanie ochronne** > dostawca, status, lokalizacja, data aktualizacji, wersja aktualizacji > data spisu

- **Lista aplikacji i oprogramowania** > dostawca, wersja aktualizacji > osoba/urządzenia uprawnione do dostępu > data spisu
- **Lista kont użytkowników, w tym czasowo nieaktywne, współdzielone, lokalne, administracyjne, itp.** > lokalizacja, status> data spisu
- **Kopia zapasowa** > status > data spisu
- **Lista podatności, luk i ataków** > lokalizacja, status, podjęte kroki na etapach reakcji i regeneracji > data spisu

Polecany link: Verve Industrial > **What is OT/ICS Asset Inventory and Why is it the Foundation of a Cyber Security Program?** (https://verveindustrial.com/resources/blog/what-is-ot-ics-asset-inventory-and-why-is-it-the-foundation-of-a-cyber-security-program/)

Erasmus+

Gdzie przechowywać spis zasobów?

Duże firmy korzystają ze specjalnych platform, jak np.:

- **Otorio** (https://www.otorio.com)
- **Axonius** (https://www.axonius.com/platform)

Obie aplikacje oferują bezpłatne demo, więc możesz je przetestować za darmo.

Możesz również sprawdzić rozwiązanie stworzone przez globalną społeczność IT:

- **CIS Controls** (https://www.cisecurity.org/controls/inventory-and-control-of-software-assets/)

To narzędzie jest bezpłatne — dostęp do niego uzyskujesz dzięki ruchowi open source. CIS Controls jest stale aktualizowany, a wśród jego twórców są firmy, agencje rządowe, instytucje i osoby prywatne z wielu branż (analitycy cybernetyczni, specjaliści ds. wynajdywania podatności, dostawcy rozwiązań, użytkownicy, konsultanci, politycy, kadra zarządzająca, środowisko akademickie, audytorzy itd.)

10. Dezaktywuj wszystkie nieużywane usługi

Dzięki spisowi zasobów możesz zarządzać nieużywanymi usługami, produktami i aplikacjami, które będą wkrótce wygasną lub już wygasły. Czy pamiętasz, ile razy wpisywałeś dane swojej firmy, w tym numer karty kredytowej, aby aktywować aplikację? No właśnie...

Jeśli więc nie reaktywujesz konta, te informacje staną dostępne dla potencjalnego hakera.

11. Zrewiduj połączenia między urządzeniami

Nie wszystkie urządzenia w firmie muszą komunikować się ze sobą wzajemnie lub z siecią. Przeanalizuj wszystkie połączenia i zdecyduj, które z nich są konieczne, a które nie.

Jeśli zarządzasz dużą bazą danych lub transakcjami finansowymi, być może lepiej byłoby to robić na jednym konkretnym komputerze, który nie ma połączenia z innymi urządzeniami firmy.

12. Określenie poziomów dostępu do danych

Tak jak nie wszystkie urządzenia muszą się ze sobą komunikować, tak nie wszyscy pracownicy muszą mieć dostęp do wszystkich danych, kont i dokumentów. Jeśli już stworzyłeś/-aś spis zasobów, możesz kontrolować swoje urządzenia i oprogramowanie. Teraz nadszedł czas na stworzenie kolejnego dokumentu, który pomoże Ci zarządzać cyberbezpieczeństwem — opis poziomu dostępu do danych.

Poziom dostępu to zestaw uprawnień lub ograniczeń nadawanych w celu uzyskania dostępu do zestawu danych.

Jeśli jesteś programistą, możesz po prostu zakodować poziomy dostępu w aplikacji lub witrynie. Jednak nie tylko programiści powinni myśleć o tworzeniu poziomów dostępu. Nawet jeśli nie masz wykształcenia informatycznego, jesteś w stanie poczynić pewne kroki.

Od czego zacząć?

Erasmus+

Poziomy dostępu do danych – podstawy

Jak już wspomnieliśmy, poziomy dostępu oparte są na zestawie uprawnień lub ograniczeń. Przede wszystkim, trzeba skategoryzować wszystkie dane, w tym aplikacje i oprogramowanie, a następnie nadać im priorytet, np.

kategoria A	najwyższy priorytet
kategoria B	wysoki priorytet
kategoria C	średni priorytet
kategoria D	niski priorytet
kategoria E	najniższy priorytet

znaczenie

Erasmus+

Poziomy te są oczywiście przykładowe. To od Ciebie zależy, ile ich będzie. Najważniejsze jest to, abyś wiedział/-a, którzy pracownicy powinni mieć dostęp do danych i na jakich zasadach.

Na przykład, wrażliwe dane, które przechowujesz w bazie danych klientów, mogą być dostępne tylko dla 2 osób, którzy pracują z nimi codziennie. W razie kryzysu dołącza do nich 2 innych pracowników. W ten sposób realizujesz jeden z punktów planu zarządzania cyberkryzysem.

W efekcie tylko kilka osób ma dostęp do tej kategorii danych. Pomyśl, jak to ułatwia zarządzanie kryzysem — jeśli wspomniane dane zostaną udostępnione poza firmę, łatwo będzie zlokalizować wyciek. Będziesz miał 4 osoby do sprawdzenia, ich urządzenia i historię działania. To dużo łatwiejsze, niż sprawdzenie wszystkich pracowników, partnerów i dostawców.

Erasmus+

Możesz stworzyć listę poziomów dostępu do danych samodzielnie lub poprosić o wsparcie eksperta ds. cyberbezpieczeństwa. Cokolwiek wybierzesz, pamiętaj, aby poinformować swoich pracowników, jaki poziom dostaną. Przeszkol ich, co te poziomy oznaczają w codziennej pracy i w sytuacji cyberkryzysu.

Pamiętaj również o regularnym aktualizowaniu listy, szczególnie wtedy, gdy któryś z Twoich pracowników zmienia stanowisko, awansuje lub odchodzi z firmy. Aktualizowanie tej listy może być jednym z obowiązków osoby (osób) odpowiedzialnej za reagowanie w sytuacjach cyberkryzysowych. Jeśli zarządzasz większym zespołem, możesz przydzielić do tego zadania inną osobę.

Może to być:

- ekspert ds. cyberbezpieczeństwa
- konsultant ds. cyberbezpieczeństwa
- analityk ds. cyberbezpieczeństwa
- admin systemów IT

13. Nie przechowuj wszystkich danych w jednym miejscu

Nie chodzi o to, że nie możesz trzymać swoich danych w jednej bezpiecznej chmurze. Chodzi o to, że jeśli niektóre kluczowe dane dotyczące Twojej firmy, takie jak dane klientów lub dane finansowe, będą zajmować jeden ekran, ułatwiasz sprawcy ataku wykonanie zrzutu ekranu w ciągu kilku sekund.

Takie dane mogą być również łatwo skradzione poprzez wykonanie zdjęcia za pomocą smartfona. Warto więc przemyśleć politykę posiadania smartfonów w firmie. Być może nie wszyscy ich potrzebują, być może nie we wszystkich miejscach.

Pamiętaj też, że zrzut ekranu pulpitu może zostać wykonany, gdy Ty lub któryś z pracowników pracuje w kawiarni, hotelowym lobby, pociągu czy na lotnisku. Przeszkol swoich pracowników, że nawet połączenie przez VPN nie chroni ich w pełni przed zhakowaniem. Twoi pracownicy zawsze muszą się chronić się.

Erasmus+

14. Korzystaj z filtrów prywatyzujących na ekrany

Jak już wspomnieliśmy, nawet VPN nie jest w stanie ochronić Twoich danych w miejscu publicznym. Dlatego polecamy Ci używanie specjalnych filtrów prywatyzujących wykonanych z TPU (termoplastyczny poliuretan) przeznaczonych do naklejania na ekrany Twoich urządzeń .

Ten materiał to chemicznie wzmocniony plastik, który charakteryzuje się odpornością na zarysowania, elastycznością, odpornością tłuszcze i smar oraz zwiększoną wytrzymałością. Dlaczego sądzimy, że tego potrzebujesz?

Ponieważ jest on również używany do produkcji filtrów na ekrany o specjalnych właściwościach. TPU zapobiega podglądaniu zawartości Twojego ekranu przez osoby patrzące na niego z boku.

Dla innych Twój ekran będzie po prostu czarny. Nie będą mogli zrobić zdjęcia jakichkolwiek danych.
Z drugiej strony Ty będziesz mógł/ mogła normalnie wykonywać swoją pracę, bo będziesz widzieć wszystko normalnie.

Polecany link: Viola Pan > **Part Three: PET, TPU, or Tempered Glass – all you need to know to choose a screen protector** (https://www.linkedin.com/pulse/part-three-pet-tpu-tempered-glass-all-you-need-know-choose-viola-vmax/)

Erasmus+

15. Ucz innych

Nie zapominaj, że cyberbezpieczeństwo nie jest działaniem jednorazowym. To długoterminowy plan, który powinien być wdrażany stopniowo i z rozmysłem. Wymaga zaangażowania wszystkich pracowników, choć niekoniecznie w ten sam sposób. Zależy to od przyjętej w firmie strategii zarządzania cyberkryzysem.

Pamiętaj także, że to ludzie są najsłabszym ogniwem Twojego systemu cyberbezpieczeństwa. Szkol swoich pracowników, informuj ich o zmianach, aktualizacjach i nowych metodach socjotechnicznych.

Gotowy/-a, by zacząć?

Erasmus+

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 therein.