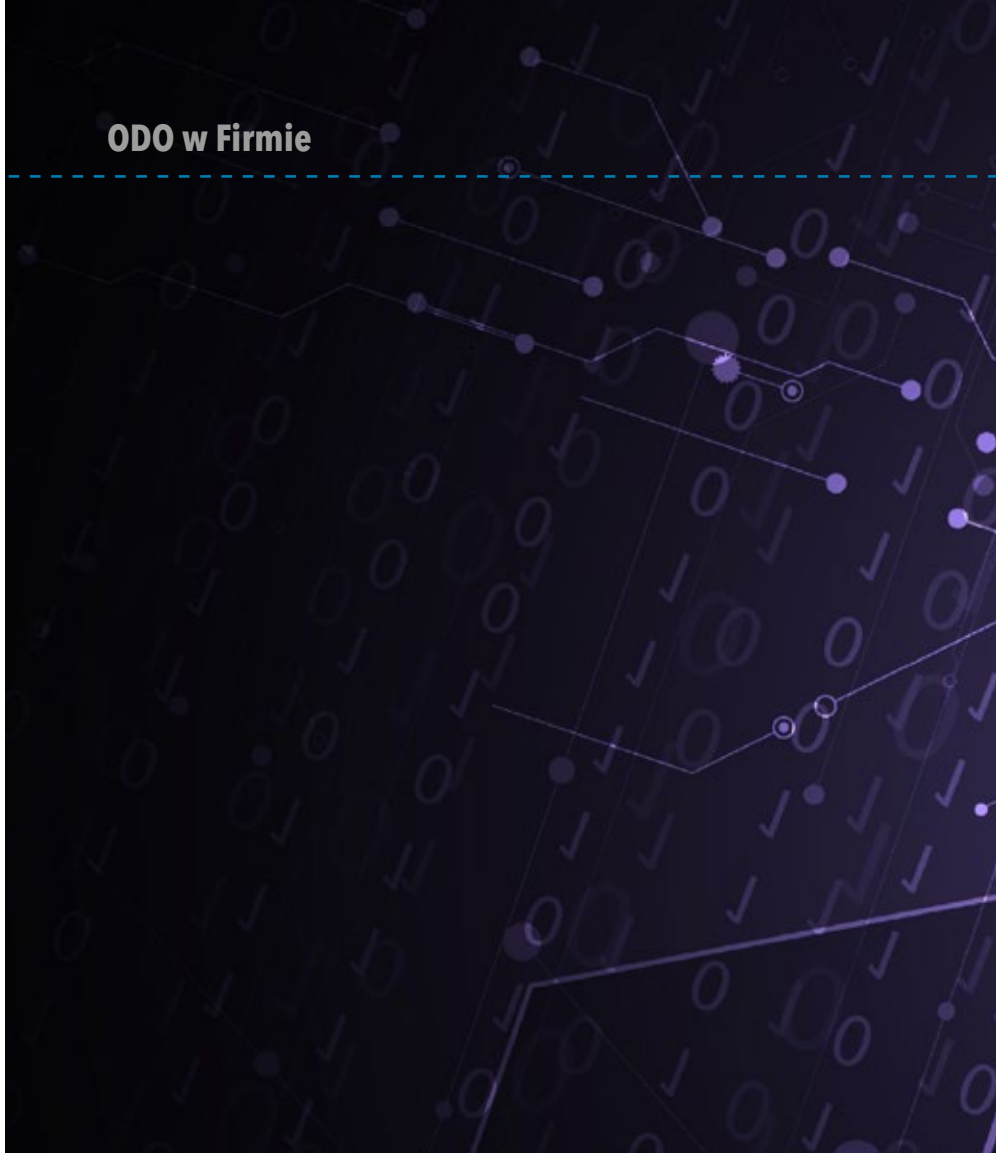
DMZ
KANCELARIA

**Michał Zadrożny**
Adwokat, posiada wieloletnie doświadczenie w zakresie obsługi prawnej klienta korporacyjnego oraz reprezentacji klientów przed sadami. Ekspert do spraw gospodarczych, z zakresu ochrony danych osobowych i cyberbezpieczeństwa. Audytor wiodący zarządzania bezpieczeństwem informacji (ISO/IEC 27001) i audytor wewnętrzny zarządzania informacjami o prywatności (ISO/IEC 27701).



# Cyberhigiena – minimalizacja ryzyka związanego z cyberzagrożeniami w Twojej firmie

Cyberbezpieczeństwo jest jednym z największych wyzwań XXI wieku, wyzwań każdej organizacji niezależenie od jej wielkości, choć wiele osób z zarządzających małymi i średnimi przedsiębiorstwami uważa, że ich ten problem nie dotyczy. Nic bardziej mylnego. Ten problem dotyczy każdej organizacji, a w zasadzie każdego użytkownika i nie tylko w sferze służbowej, ale i prywatnej. Dzisiaj żyjemy w globalnej, niebezpiecznej wiosce połączonej siecią Internet z zagrożeniami na każdym skrzyżowaniu dróg.

Z uwagi na ogólnoświatową pandemie i rozprzestrzenianie się choroby COVID-19 wiele organizacji musiało zmienić z dnia na dzień organizację pracy i przejść na prace zdalną. Niestety duża część organizacji i ich pracownicy nie byli na to gotowi, co oczywiście również zostało wykorzystane przez cyberprzestępców w postaci zwiększenia się ataków socjotechnicznych na użytkowników. To człowiek jest najsłabszym ogniwem każ-

dego systemu i należy zrozumieć, że to człowiek będący użytkownikiem jakiejkolwiek technologii informatycznej ma największy wpływ na minimalizację cyberzagrożeń. W tym celu niezbędna jest świadomość użytkowników.

Cyberbezpieczeństwo to nie tylko kwestia związana z technologią, ale kwestia, w przypadku której równie ważne są ludzkie zachowania. W związku z powyższym organizacje nie tylko muszą inwestować w zabezpieczenia techniczne, ale również w budowanie świadomości pracowników, którzy korzystają na co dzień z różnych technologii informatycznych. Należy pamiętać, że nie jest możliwe zbudowanie świadomości użytkownika jednym szkoleniem – żeby szkolenia miały efekt muszą być systematyczne i w mojej ocenie nie rzadsze niż raz w roku. Duże przedsiębiorstwa co do zasady o tym wiedzą, teraz czas na małe i średnie.

Niestety pomimo budowania świadomości, pracownicy i tak będą popełniali błędy, będą budowali proste hasła, czy wykorzystywali te same hasła w życiu służbowym i prywatnym. Starajmy się te błędy minimalizować choćby poprzez wdrażanie właściwych i adekwatnych zabezpieczeń w postaci polityk haseł, czy stosowanie w jak najszerszym stopniu uwierzytelniania dwuskładnikowego (2FA). Jednakże pomimo wdrożenia zaawansowanych zabezpieczeń technicznych (np. technologii DLP[1]) incydenty bezpieczeństwa, w tym naruszenia danych osobowych będą się zdarzały.

## Cyberhigiena. Co to takiego?

W czasie pandemii staramy się stosować powszechne zasady higieny, ale musimy zacząć również stosować cyberhigienę. W świecie technologii informatycznej też czekają na nas zagrożenia. Cyberhigena nie jest pojęciem nowym, choć unijny ustawodawca zdefiniował cyberhigienę dopiero 17 kwietnia 2019 roku w akcie o cyberbezpieczeństwie, tj. Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2019/881. Cyberhigiena to proste, rutynowe czynności, których wdrożenie i regularne wykonywanie przez obywateli, organizacje i przedsiębiorstwa minimalizuje ich narażenie na ryzyka związane z cyberzagrożeniami. Wydaje się proste, ale diabeł tkwi w szczegółach. Na po-

[1] Technologii DLP ma na celu ochronę danych w postaci elektronicznej przed kradzieżą lub przypadkowym „wyciekiem".

ziomie UE za propagowanie najlepszych praktyk i rozwiązań w zakresie cyberbezpieczeństwa, w tym cyberhigieny odpowiedzialna jest ENISA, czyli Agencja Unii Europejskiej ds. Cyberbezpieczeństwa[2]. Agencja ta jest dla większości z nas znana. Swoją „rozpoznawalność w szerszym gronie" zyskała dzięki zaleceniom dotyczącym metodyki oceny wagi naruszeń danych osobowych[3], które to są niezwykle przydatne do oceny naruszeń ochrony danych na gruncie RODO (vide: art. 33 i 34 RODO).

ENISA po analizie wybranych programów higieny cybernetycznej Unii Europejskiej oraz analizie wybranych małych i średnich przedsiębiorstw w lutym 2017 roku opublikowała raport[4]: Review of Cyber Hygiene practices. Pomimo, że raport ma przeszło trzy lata jest co do zasady aktualny. ENISA w raporcie wskazała zadania jakie w ocenie agencji należy podjąć w celu zbudowania skutecznego systemu cyberhigieny w małych i średnich organizacji.

## ENISA: 10 podstawowych zadań w zakresie cyberhigieny

Podstawowe zadania w zakresie cyberhigieny to:

1. Przeprowadzenie inwentaryzacji całego sprzętu, w celu zbudowania świadomości o zasobach, które posiada organizacja;

2. Przeprowadzenie inwentaryzacji całego posiadanego oprogramowania i zweryfikowanie jego aktualności.

Należy okresowo weryfikować, czy zainstalowane oprogramowanie na komputerach czy telefonach służbowych personelu jest nadal potrzebne użytkownikowi i zaleca się usuwanie zbędnego oprogramowania. Jednakże to aktualizowanie oprogramowania jest fundamentem cyberbezpieczeństwa organizacji. Duża część masowych cyberataków ostatnich lat (np. ransomware) wykorzystywała podatności, które zostały wcześniej udokumentowane, a dostawcy oprogramowania wydali już stosowane aktualizacje bezpieczeństwa. Należy pamiętać o aktualizacji nie tylko systemów operacyjnych, ale również urządzeń wykorzystywanych w lokalnej sieci, zwłaszcza routerów dostępowych.

Należy okresowo weryfikować, czy zainstalowane oprogramowanie na komputerach czy telefonach służbowych personelu jest nadal potrzebne użytkownikowi i zaleca się usuwanie zbędnego oprogramowania. Jednakże to aktualizowanie oprogramowania jest fundamentem cyberbezpieczeństwa organizacji. Duża część masowych cyberataków ostatnich lat (np. ransomware) wykorzystywała podatności, które zostały wcześniej udokumentowane, a dostawcy oprogramowania wydali już stosowane aktualizacje bezpieczeństwa. Należy pamiętać o aktualizacji nie tylko systemów operacyjnych, ale również urządzeń wykorzystywanych w lokalnej sieci, zwłaszcza routerów dostępowych. Poza tym rekomenduje się korzystanie z wiarygodnych dostawców – nie ma darmowych usług w świecie IT. Jeżeli nie jest się klientem, to zazwyczaj jest się produktem lub używa się oprogramowania niezgodnie z warunkami licencyjnymi;

3. Korzystanie z dostarczanych przez producentów posiadanych systemów IT instrukcji bezpiecznej konfiguracji oraz procedur harderingu, czyli między innymi list kontrolnych zawierających rekomendowane zmiany w konfiguracji;

4. Odpowiednie zarządzanie danymi w sieci wewnętrznej i poza nią;

5. Skanowanie wszystkich przychodzących wiadomości e-mail;

6. Ograniczenie do minimum kont administracyjnych;

7. Regularne tworzenie i testowanie kopii zapasowych danych.

Niestety wiele małych i średnich organizacji popełnia podstawowe błędy w przechowywaniu kopii danych np. wykonuje je lokalnie i przechowuje je w tej samej strefie pożarowej, czy posiada tylko jeden zestaw kopii bezpieczeństwa;

8. Opracowanie planu reagowania na incydenty;

9. Egzekwowanie podobnych zasad bezpieczeństwa u wszystkich dostawców;

10. Zapewnienie we wszystkich umowach serwisowych odpowiednich środków kontroli bezpieczeństwa.

Wdrożenie wszystkich dziesięciu rekomendacji bez własnych służb informatycznych może być wyzwaniem dla przedsiębiorstwa, ale które należy podjąć. Niestety wiele przedsiębiorstw, które posiada własne służby IT nie wdrożyło powyższych rekomendacji. Jest to zjawisko niepokojące biorąc pod uwagę codzienne zagrożenia dla organizacji, których zmaterializowanie może doprowadzić do nieodwracalnych konsekwencji dla dalszego funkcjonowania przedsiębiorstwa.

---

[2] Aktem o cyberbezpieczeństwie ENISA nie tylko zmieniła nazwę z Europejskiej Agencji Bezpieczeństwa Sieci i Informacji na Agencja Unii Europejskiej ds. Cyberbezpieczeństwa ale również nastąpiło wzmocnienie roli tejże agencji m.in. o koordynację europejskiej współpracy operacyjnej w zapewnieniu bezpieczeństwa europejskiej cyberprzestrzeni.

[3] https://www.enisa.europa.eu/publications/dbn-severity/

[4] https://www.enisa.europa.eu/publications/cyber-hygiene