ZWARCI, SILNI, GOTOWI?

POLSKIE FIRMY W OBLICZU CYBERZAGROŻEŃ

RAPORT

CyberDefence 24

DGTL

CyberDefence 24

KIBIL PIECUCH I WSPÓLNICY

Warszawa 2022


CRITICAL ERROR
ALL PROCESS TERMINATED
CRITICAL ERROR
ALL PROCESS TERMINATED

Raport

Zwarci, silni, gotowi? Polskie firmy w obliczu cyberzagrożeń.

SPIS TREŚCI

Nikola Bochyńska
Redaktor Naczelna CyberDefence24.pl

“Zwarci, silni, gotowi” – tytuł raportu sugeruje modelowe podejście osób zarządzających polskimi firmami do kwestii cyberbezpieczeństwa w ich organizacjach. Życzylibyśmy sobie, aby tak było. Ostatnie ponad dwa lata nauczyły nas - nie tylko pod względem bezpieczeństwa danych i systemów - że musimy zachować czujność w każdej sekundzie. Poczucie braku stabilności czy możliwości przewidzenia, co wydarzy się zarówno w skali lokalnej, jak i globalnej, to z jednej strony zagrożenie, a z drugiej szansa, by wyciągnąć wnioski i lepiej przygotować się na różne scenariusze. Nigdy nie możemy być w 100 procentach pewni, że jesteśmy bezpieczni w sieci, dlatego zawsze bądźmy w stanie podwyższonej gotowości i nastawieni, że w każdej chwili może mieć miejsce incydent cyberbezpieczeństwa. Jak pokazało wiele przykładów z Polski i świata – adwersarz nigdy nie śpi.

Gen. bryg. Karol Molenda, Dowódca Komponentu Wojsk Obrony Cyberprzestrzeni, powtarza, że „cyberbezpieczeństwo to gra zespołowa”. Podobnie, jak firmy nie da się budować samodzielnie, a w oparciu o zgrany zespół, tak warto pamiętać, że aby polska cyberprzestrzeń była bezpieczna, potrzebna jest nie tylko sporadyczna współpraca, ale udana synergia obu sektorów: publicznego i prywatnego.

W wyścigu o specjalistów, których ciągle nam brakuje często zapominamy, że mamy wspólny cel. Być może zatem warto połączyć siły?

Każdy czyn niesie z sobą określone konsekwencje. Miejmy nadzieję, że ostatnie dwa lata, w tym m.in. mnogość cyberincydentów, a także trwająca wojna w Ukrainie (również w sferze cyber) sprawią, że polskie firmy będą gotowe na każdą ewentualność.

Dziś nikomu już nie trzeba powtarzać, że cyberbezpieczeństwo ma znaczenie. Czy zarządzający polskimi firmami są o tym przekonani? Tego dowiecie się Państwo z lektury tego raportu, do czego serdecznie zapraszamy.

Irek Piecuch
Senior Partner DGTL Kibil Piecuch I Wspólnicy

„Jaki koń jest każdy widzi?"
Benedykt Chmielowski, Nowe Ateny, Lwów 1745

Definicja konia autorstwa Benedykta Chmielowskiego weszła do kanonu polskich powiedzeń. Przez lata stała się synonimem czegoś oczywistego. A jak się sprawy mają z cyberbezpieczeństwem? Czy termin ten wszedł już na stałe do obiegu w polskim przedsiębiorstwach? Czy stał się elementem uwzględnianym w projektowaniu governance firmy, budowania jej struktury, projekcji finansowych? Jaką wagę polskie firmy przywiązują do tego zagadnienia?

Na te między innymi pytania, miało odpowiedzieć badanie przeprowadzone wspólnie przez zespół kancelarii DGTL oraz redakcji Cyberdefense24 wśród grona ponad pięćdziesięciu polskich przedsiębiorstw. Stosunkowo wąskie grono badanych firm, nie pozwala co prawda na wyciąganie wniosków które mógłby być reprezentatywne dla konkretnych grup przedsiębiorstw, ale z pewnością stanowić będzie ciekawy materiał do przemyśleń dla wszystkich, którzy zadają sobie obecnie pytanie czy i jak powinni uwzględnić cyberbezpieczeństwo w praktyce codziennego funkcjonowania swoich firm.

Dane gromadzone przez przedsiębiorstwa coraz częściej stanowią o ich wartości i przewadze konkurencyjnej. Transformacja cyfrowa dla wielu z nich oznacza powiązanie sukcesu firmy z dostępnością i wydajnością infrastruktury teleinformatycznej. Możliwość przełamania środków bezpieczeństwa przedsiębiorstwa i dopuszczenia do niekontrolowalnego wypływu zgromadzonych danych, może łączyć się nie tylko z utratą poufnych informacji dotyczących produktów czy też strategii firmy, ale także z dopuszczeniem do ujawnienia danych osobowych klientów firmy. To z kolei może pociągać za sobą wielomilionowe kary, utratę zaufania tych ostatnich oraz szkody na wizerunku marki.

Dane oraz ich bezpieczeństwo oznaczają zatem dla współczesnych przedsiębiorstw z jednej strony możliwość uzyskania szybkich wzrostów, wysokiej wyceny i konkurencyjności na rynku. Z drugiej zaś strony ryzyko utraty setek milionów w przeciągu kilku tygodni. Takie cyfrowe Yin i Yang. Jak zatem wygląda cyberbezpieczeństwo w praktyce działania polskich firm? Jak firmy te podchodzą do wyzwań związanych z cyberbezpieczeństwem? Mamy nadzieję, że lektura naszego raportu odpowie przynajmniej na niektóre z tych pytań.

PODZIĘKOWANIA

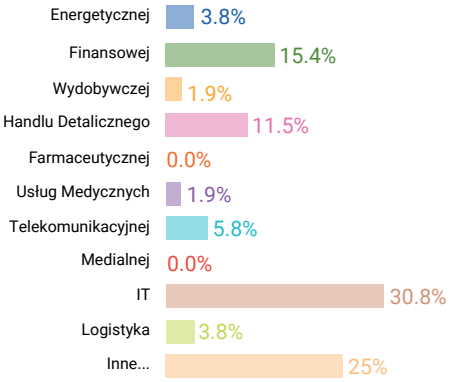
Pomimo napiętych grafików nasi respondenci znaleźli czas, by podzielić się swoimi doświadczeniami. Dlatego też chcielibyśmy wyrazić nasze głębokie podziękowania dla wszystkich osób z 52 firm, które zdecydowały się wziąć udział w naszym badaniu.

Z uwagi na wrażliwe dane, jakie mogą zostać wyczytane z Raportu odstąpiliśmy od wskazywania nazw firm, które wzięły udział w Raporcie.

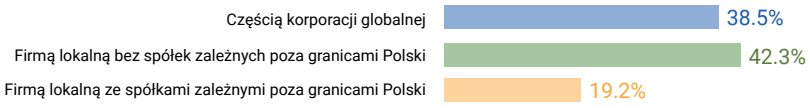
I. Informacje podstawowe

1. Reprezentuje Pan/Pani przedsiębiorstwo z sektora:

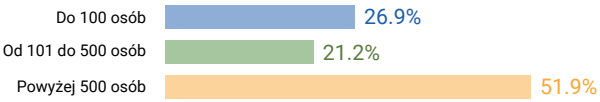
2. Firma działa w branży:



3. Państwa przedsiębiorstwo jest:



4. Państwa przedsiębiorstwo zatrudnia (bez względu na formę prawną zatrudnienia):



Ankiety do raportu zostały przeprowadzone w okresie od 4 lutego 2022 r. do 24 marca 2022 r. z 52 przedsiębiorstwami reprezentowanymi przez członków zarządu odpowiedzialnych za cyberbezpieczeństwo, szefów działów IT, bezpieczeństwa lub cyberbezpieczeństwa oraz działów prawnych.

Ponad 80% ankietowanych reprezentowała sektor prywatny. Większość respondentów (30,8%) reprezentowała firmy z branży IT. Wśród ankietowanych znajdowały się także firmy reprezentujące branżę energetyczną, finansową, wydobywczą, usług medycznych, telekomunikacyjną, ubezpieczeniową, logistyczną, handlu detalicznego, hazardową a także sektor zbrojeniowy.

Niektórych z firm nie dało się jasno sklasyfikować pod jedną kategorię działalności.

Niecałe 40% respondentów reprezentowało firmy będące częścią korporacji globalnej. Firmy nie posi-

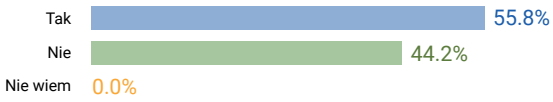
adające spółek zależnych poza granicami Polski reprezentowało 42% respondentów, a prawie 20% z nich reprezentowało firmy lokalne ze spółkami zależnymi poza granicami Polski.

Ponad połowa respondentów reprezentowała firmy zatrudniające powyżej 500 osób. Niektóre z nich zatrudniały ponad 10 tysięcy osób na świecie.

Badania w przeważającej większości zostały przeprowadzone za pośrednictwem wideokonferencji. Pozostała część polegała na wypełnieniu ankiety przez respondentów. Raport stanowi podsumowanie zebranych wypowiedzi ankietowanych, bez przypisywania ich do konkretnej firmy czy branży.

II. Informacje podstawowe z zakresu cyber

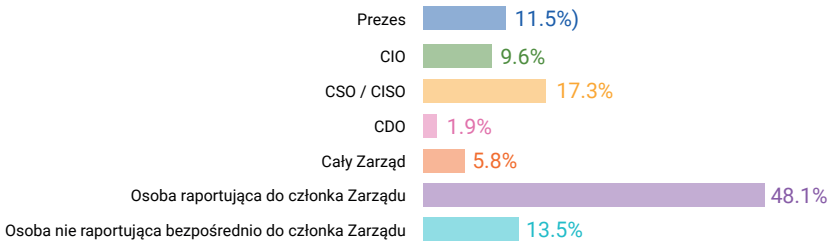
5. Czy Państwa organizacja podlega pod regulacje ustawy o krajowym systemie cyberbezpieczeństwa lub inne branżowe przepisy w zakresie cyberbezpeczeństwa?



Kiedy ustawa o Krajowym Systemie Cyberbezpieczeństwa („UKSC") wchodziła w życie, jednym z częściej pojawiających się zarzutów było to, że miała stosować się do dość wąskiego kręgu podmiotów, choć i tak do końca nie było wiadomo czy liczba tych podmiotów wyrażać się będzie w setkach czy może w tysiącach. Oczywistym było jednak to, że będzie to ułamek całej branży.

W naszym badaniu ponad połowa respondentów (55,8%) podlega przepisom ustawy lub przepisom branżowym poświęconym cyberbezpieczeństwu.

6. Kto odpowiada za kwestię cyberbezpieczeństwa w Państwa firmie?



Przez lata utarło się, że bezpieczeństwo firmy jest kwestią ważną, ale z wyjątkiem specyficznych branż, z rzadka tylko zaliczaną do ryzyk krytycznych, jeżeli chodzi o funkcjonowanie i rozwój danego przedsiębiorstwa. Wydaje się, że w wielu firmach cyberbezpieczeństwo (przynajmniej początkowo) zakwalifikowano jako część szerszego, od dawna istniejącego już zagadnienia, co znalazło swoje odbicie zarówno w strukturze organizacyjnej (część działu bezpieczeństwa lub działu IT) jak i konstrukcji budżetu (brak wyodrębnionego i dedykowanego budżetu).

Postępująca transformacja cyfrowa gospodarki, zwiększające się uzależnienie od ilości i jakości przetwarzanych danych a także rozbudowa środowiska regulacyjno-prawnego sprawiają, że takie podejście może okazać się niewłaściwe. Ryzyko wynikające z możliwości wystąpienia incydentów w obszarze cyberbezpieczeństwa, zwiększa się z roku na rok, co powoduje konieczność ponownej rewizji mapy ryzyk oraz istniejących w przedsiębiorstwie procesów dotyczących zarządzania bezpieczeństwem informacji.

Żeby to zobrazować warto przytoczyć przykład firmy, która stała się synonimem cyfrowego wzrostu - spółki Equifax. Pomiędzy majem a lipcem 2017 roku łupem hackerów padły dane przechowywane przez ta spółkę a należące do 147,9 milionów amerykanów. Co ciekawe, na trzy miesiące przed atakiem, na rynku pojawiła się informacja o podatności oprogramowania open-source wykorzystywanego przez Equifax na ryzyko zhackowania. Firma nie zareagowała, pomimo tego, że próby wykorzystania tej podatności były odnotowywane niemal równolegle z jej odkryciem. Nie zadziałały także właściwie mechanizmy wykrywania nieprawidłowości wykorzystywane przez Equifax. Minęło długich 76 dni zanim wykryto incydent. Dwa lata po tych wydarzeniach, w oficjalnych raportach finansowych Equifax przyznał, że łączny koszt działań firmy wywołanych incydentem przekroczył 1,35 miliarda dolarów.

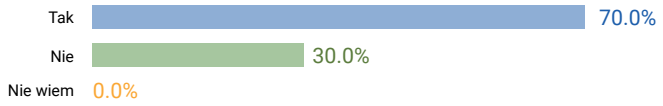
Badania firmy IBM pokazują, że średnie szkody wyrządzone atakiem na infrastrukturę informatyczną firmy rosną nieustannie od roku 2017 i zgodnie najnowszym raportem tej firmy „Cost of a Data Breach 2021" osiągnęły już pułap 4,24 milionów dolarów (z czego prawie 40 procent to utracony przez firmy biznes).

Na horyzoncie widać już projekt Dyrektywy określanej jako NIS II, która ma w istotny sposób zaostrzyć reżim regulacyjny, powiększyć uprawnienia regulatora i wprowadzić reżim kar na poziomie podobnym do kar, które mogą być obecnie nakładana za naruszanie zasad przetwarzania danych osobowych.

Przeprowadzona ankieta wskazuje, że w połowie przypadków, osoba odpowiedzialna za kwestie cyberbezpieczeństwa nie jest członkiem zarządu firmy. Jedynie w 12% przypadków osobą taką jest Prezes firmy. Pozostałe opcje to Chief Information Officer („CIO"), Chief Security Officer ("CSO"), Chief Information Security ("CISO") oraz Chief Data Officer ("CDO") (zaledwie w 2% sytuacji). W 14% firm osoba odpowiedzialna za kwestie cyberbezpieczeństwa nie raportuje bezpośrednio do członka Zarządu.

Uzyskane wyniki wskazują wyraźnie, że na rynku brak jest obecnie, jednej dominującej wizji organizacji obszaru zajmującego się cyberbezpieczeństwem firmy.

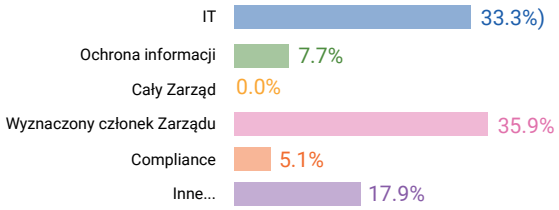
7. Czy w Państwa firmie została wyodrębniona struktura organizacyjna odpowiedzialna za cyberbezpieczeństwo?



Zgodnie z art.14 UKSC operator usługi kluczowej w celu realizacji zadań nałożonych na niego przez ustawę zobowiązany jest powołać wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo. Może też ewentualnie, zawrzeć umowę z podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa. Zgodnie z ustawą, wewnętrzne struktury powołane przez operatora usługi kluczowej odpowiedzialne za cyberbezpieczeństwo oraz podmioty świadczące usługi z zakresu cyberbezpieczeństwa są obowiązane spełniać warunki organizacyjne i techniczne pozwalające na zapewnienie cyberbezpieczeństwa obsługiwanemu operatorowi usługi kluczowej, dysponować odpowiednio przygotowanymi pomieszczeniami a także stosować zabezpieczenia w celu zapewnienia poufności, integralności, dostępności i autentyczności przetwarzanych informacji, z uwzględnieniem bezpieczeństwa osobowego, eksploatacji i architektury systemów.

Wysoki odsetek respondentów potwierdzających utworzenie wewnętrznej struktury odpowiedzialnej za cyberbezpieczeństwo (przy jednoczesnej informacji, iż jedynie połowa z nich podlega ustawie), wskazuje na to, że rozwiązanie to, przyjmują także firmy, których UKSC nie objęła. Jednocześnie prawie jedna trzecia badanych firm, nie dysponuje własnym, wyodrębnionym zespołem, co może pozostawać w korelacji z wielkością firm (26,9% badanych firm zatrudnia poniżej 100 osób) lub z przyjętym modelem biznesowym (outsourcing).

8. Jeżeli struktura taka została wyodrębniona to pod jaki dział lub departament podlega?

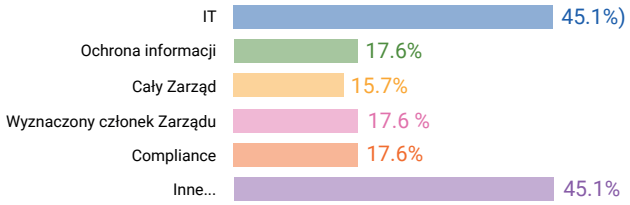


Cyberbezpieczeństwo bardzo często sprowadzane jest do kwestii IT. Stąd też, dość częsta asocjacja z działem IT. W wielu przypadkach rozwiązanie takie może być jednak problematyczne, albowiem zapewnienie cyberbezpieczeństwa firmy związane jest z wieloma aspektami jego działalności (nie tylko IT). Co więcej może się okazać, że podleganie takiej struktury pod dział IT rodzić będzie szereg konfliktów interesów (rozwój infrastruktury czy usług IT vs. potencjalne zagrożenia), których znaczenie znacznie wykracza poza same struktury IT. Wyniki ankiety pokazują, że rozwiązaniami najczęściej stosowanymi jest podległość pod dział IT (33,3%) lub bezpośrednio pod określonego członka Zarządu firmy (35,9%).

9. Jeżeli struktura taka została wyodrębniona to czy dysponuje ona swoim odrębnym budżetem?

Kiedy w roku 2015 Najwyższa Izba Kontroli wydała raport dotycząca działań administracji rządowej w obrębie cyberbezpieczeństwa, jednym z głównych zarzutów był brak wyasygnowania odpowiednich środków finansowych na realizację zadań w tym zakresie. Nakłady organizacji przestępczych realizujących swój proceder w cyberprzestrzeni, na rozwój oprogramowania złośliwego oraz nowych metod ataków wycenia się w miliardach dolarów. Z drugiej strony, wiele firm traktuje nakłady na cyberbezpieczeństwo jako koszt nie związany bezpośrednio z uzyskiwanymi przychodami. Jedynie około 60% badanych firm alokuje odrębne środki finansowe na działania związane z cyberbezpieczeństwem, co oznacza, że pozostałe 40% musi sięgać do budżetów innych działów, mających szereg innych priorytetów. Oczywiście wydzielenie budżetu nie jest elementem koniecznym, ale w praktyce utrudnia realizowanie długofalowej strategii budowania odporności przedsiębiorstwa w badanym obszarze.

10. Czy Państwa organizacja posiada certyfikacje odnoszące się do obszaru – np. certyfikacje dotyczące bezpieczeństwa zarządzania informacją:



Wedle wyników naszych badań prawie 70% przedsiębiorców wprowadziło Business Continuity Plan (BCP), co należy ocenić pozytywnie, przy założeniu, że poziom świadomości cyberbezpieczeństwa stale wzrasta i organizacje będą ten element nie tylko uzupełniać, ale i nim zarządzać.

Niepokojącym zjawiskiem jest fakt, że 11,5% respondentów nie miało wiedzy, czy w ich organizacjach w ogóle wprowadzono BCP. Na tą odpowiedź zwracamy uwagę, ponieważ bardzo trudno wyobrazić sobie skuteczne zabezpieczenie ciągłości działania w sytuacji, w której część zarządzających nie wie o istnieniu BCP. Jak zatem ten plan wykonać? Natomiast u 19,2% z badanych przedsiębiorców BCP nie wprowadzono w ogóle, co niewątpliwie wymaga uwagi w przyszłości.

Powyższe znajduje potwierdzenie także w wynikach raportu Computerworld „Inwestycje IT w kierunku rozwoju polskich firm w latach 2021-2022”1, z którego wyłania się niebagatelna rola chmury jako czynnika zwiększającego poziom bezpieczeństwa polskich firm, a tym samym ich zdolności do zabezpieczenia ciągłości działania. Aż 57% respondentów wymienionego raportu planuje wdrażać rozwiązania chmurowe w celu podniesienia bezpieczeństwa infrastruktury, tak aby zapewnić ciągłość działania biznesu.

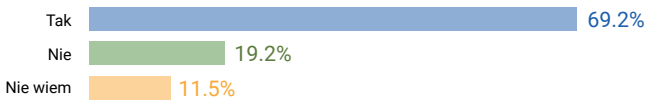
Rola BCP nie pozostaje także bez znaczenia w prowadzeniu audytów w sektorze regulowanym, podlegającym nadzorowi, chociażby nadzorowi Urzędu Komisji Nadzoru Finansowego.
Przykład z sektora finansowego; ciągłość działania

Dla niektórych podmiotów z sektora finansowego, np. Małej Instytucji Płatniczej, czy bardziej zaawansowanych instytucji finansowych, posiadanie takiego planu jest nie tylko dobrą praktyką, ale i wymogiem prawnym. Składając wniosek o wpis do rejestru dostawców usług płatniczych i wydawców pieniądza elektronicznego wnioskodawca będzie musiał załączyć do wniosku opis rozwiązań zapewniających ciągłość działania. Składając zaś wniosek o wpis do rejestru Małych Instytucji Płatniczych nie spotkamy się z wymogiem dołączania BCP do wniosku, ale już z mocy prawa wynika obowiązek MIP do posiadania procedur zarządzania ryzykiem2, w których powinno znaleźć się miejsce na BCP.

1 *Inwestycje IT w kierunku rozwoju polskich firm w latach 2021-2022. Chmura i nowe technologie”, raport Computerworld*
2 *Art. 117h ust. 2 Ustawy o usługach płatniczych z dnia 19 sierpnia 2011 r. (Dz.U. Nr 199, poz. 1175 z późn. zm.)*

Pozostając w obrębie sektora finansowego, warto zwrócić uwagę na projektowane rozporządzenie DORA (w sprawie operacyjnej odporności sektora finansowego). DORA odpowiada, m.in. na uwagi Europejskiego Urzędu Nadzoru Bankowego w przedmiocie ujednolicenia wymagań na jednolitym i europejskim rynku. I tak projektodawcy wychodzą z założenia, że odpowiedzią na coraz to szersze spektrum cyberzagrożeń jest utworzenie i utrzymywanie odpornych systemów i narzędzi ICT. A środkiem do zapewnienia wspomnianej odporności jest chociażby zdolność do szybkiego przywrócenia gotowości do pracy po wystąpieniu sytuacji nietypowej, a zatem jest to nic innego jak zadbanie o ciągłość działania.

11. Czy w Państwa firmie wdrożone BCP (Business Continuity Process / Planning)?



12. Czy Państwa firma dysponuje procedurą oraz procesem szacowania ryzyka dotyczącymi prowadzonej przez Państwa działalności?

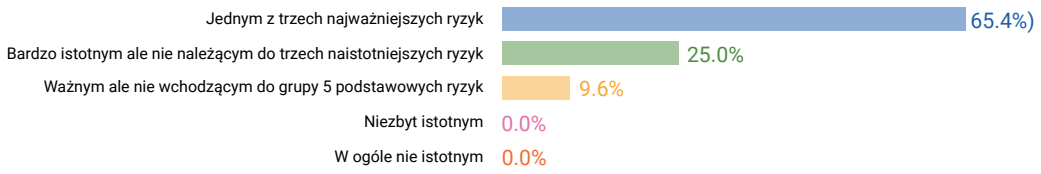
Zagadnienie dotyczące ciągłości działania koresponduje z szerszym tematem szacowania ryzyka dotyczącym prowadzenia działalności. Wedle wyników Raportu aż 86,5% organizacji dysponuje procedurą oraz procesem szacowania ryzyka dotyczącym prowadzonej przez nią działalności. Równie optymistycznym w tym kontekście jest fakt, że żaden respondent nie stwierdził, że nie wie, czy jego organizacja takie procedury posiada.

W szacowaniu ryzyka m.in. w sektorze ICT znaczenie będą miały metody wypracowane przez audytorów ISO, np. w zakresie normy ISO 27001 (bezpieczeństwo informacji) czy normy ISO 22301 (ciągłość działania biznesu), ale i stanowiskach oraz raportach ENISA (Agencja Unii Europejskiej ds. Cyberbezpieczeństwa), np. w kompendium ENISA w sprawie wzorów zarządzania ryzykiem[3]. W tym kompendium ENISA omawia normę ISO 27005[4] zawierającą wytyczne dotyczące dobrych praktyk w zakresie zarządzania ryzykiem dla informacji i wskazuje tę normę jako wspierającą zasady bezpieczeństwa informacji z normy ISO 27001. W zakresie tej normy szacowanie ryzyka może być dokonywanie przy wykorzystywaniu metod jakościowych, ilościowych lub hybrydowych.

Norma ISO 27001 dotycząca bezpieczeństwa informacji zyskała na popularności z powodu doniosłego znaczenia procesu, którego dotyczy. To znajduje również potwierdzenie w wynikach naszego badania: najbardziej popularną certyfikacją jest właśnie ISO 27001 – 45,1% przedsiębiorców posiada certyfikację z tej normy. Na kolejnych pozycjach plasuje się ex aequo: omawiane BCP (ISO 22301) – z wynikiem 17,6% oraz 17,6% certyfikacja normy ISO 27018 z zakresów danych osobowych. ENISA zaś omawia łącznie kilkadziesiąt różnych metodologii, sięgając po rozwiązania pochodzące z USA, Singapur, czy Irlandii. Na próżno jednak szukać wskazania metodologii najlepszej.

3 *Compendium of Risk Management Frameworks with Potential Interoperability*
4 *https://www.iso.org/standard/75281.html (dostęp z dnia 05.04.2022 r.)*

13. Jak istotnym ryzykiem z punktów widzenia Państwa działalności jest cyberbezpieczeństwo?



65,4% z naszych respondentów wskazało, że cyberzagrożenia są jednym z trzech najważniejszych ryzyk w ich działalności, a 25% respondentów określiło, że jest to ryzyko bardzo istotne, ale nie należy do trzech najistotniejszych. 9,6% badanych wskazało, że cyberbezpieczeństwo jest ważne, ale nie wchodzi do katalogu 5 podstawowych ryzyk działalności. Natomiast żaden ankietowany nie wskazał, że cyberbezpieczeństwo jest niezbyt istotnym lub w ogóle nie istotnym zagadnieniem.

Potwierdza to jak bardzo aktualnie firmy są uzależnione od infrastruktury IT. W przypadku zablokowania firmie dostępu do tej infrastruktury, występuje wysokie prawdopodobieństwo wstrzymania wszelkiej pracy przez firmę.

14. Czy gdyby Państwa organizacja planowałaby przejęcie innego przedsiębiorstwa, to czy elementem ceny byłby poziom zabezpieczeń produktów lub usług albo poziom cyberbezpieczeństwa całej organizacji?

Ponadto wskazać należy, że temat cyberbezpieczeństwa ma znaczenie dla biznesu także w kontekście podejmowania decyzji inwestycyjnych, a w tym przejmowania innych przedsiębiorstw. Prawie 81% badanych w naszym Raporcie odpowiedziało, że gdyby ich organizacja planowała przejęcie innego przedsiębiorstwa, to elementem wyceny byłby poziom zabezpieczeń produktów lub usług, a nawet poziom cyberbezpieczeństwa całej organizacji. Ten wynik jest także zadawalający z punktu widzenia świadomości roli cyberbezpieczeństwa już nie tyko w ciągłości działania przedsiębiorców, ale i wzrostu ich innowacyjności czy wartości danego biznesu w ujęciu kompleksowym.

Podsumowanie rozdziału II.

- W połowie przypadków, osoba odpowiedzialna za kwestie cyberbezpieczeństwa nie jest członkiem zarządu firmy. Jedynie w 12% przypadków osobą taką jest Prezes firmy. W 14% firm osoba odpowiedzialna za kwestie cyberbezpieczeństwa nie raportuje bezpośrednio do członka Zarządu.

- Na rynku brak jest obecnie, jednej dominującej wizji organizacji obszaru zajmującego się cyberbezpieczeństwem firmy.

- Prawie ¾ respondentów potwierdza utworzenie wewnętrznej struktury organizacyjnej odpowiedzialnej za cyberbezpieczeństwo w ich firmie. Potwierdza to, że respondenci respektują zagrożenia wynikające z otaczającej nas rzeczywistości.

- Wyniki ankiety pokazują, że rozwiązaniami najczęściej stosowanymi jest podległość kwestii związanych z cyberbezpieczeństwem pod dział IT lub bezpośrednio pod określonego członka Zarządu firmy.

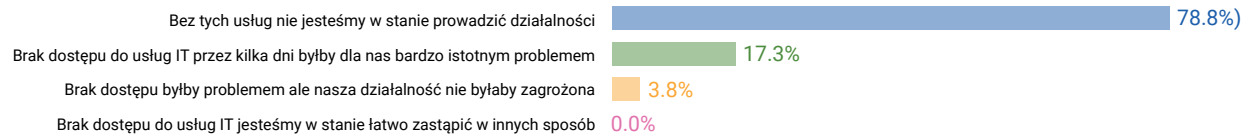
- Jedynie około 60% badanych firm alokuje odrębne śroki finansowe na działania związane z cyberbezpieczeństwem, co oznacza, że pozostałe 40% musi sięgać do budżetów innych działów, mających szereg innych priorytetów. Prawie 70% przedsiębiorców wprowadziło Business Continuity Plan (BCP), co należy ocenić pozytywnie, przy założeniu, że poziom świadomości cyberbezpieczeństwa stale wzrasta i organizacje będą ten element nie tylko uzupełniać, ale i nim zarządzać

- Dwie trzecie respondentów wskazało, że cyberzagrożenia są jednym z trzech najważniejszych ryzyk w ich działalności, a 25% respondentów określiło, że jest to ryzyko bardzo istotne, ale nie należy do trzech najistotniejszych. Żaden ankietowany nie wskazał, że cyberbezpieczeństwo jest niezbyt istotnym lub w ogóle nie istotnym zagdnieniem. Potwierdza to wysoki wpływ cyberzagrożeń na codzienną działalność biznesową firm.

- Prawie 81% badanych w naszym Raporcie odpowiedziało, że gdyby ich organizacja planowała przejęcie innego przedsiębiorstwa, to elementem wyceny byłby poziom zabezpieczeń produktów lub usług, a nawet poziom cyberbezpieczeństwa całej organizacji. Ten wynik jest także zadawalający także z punktu wzrostu innowacyjności czy wartości danego biznesu w ujęciu kompleksowym.

III. Obecność w sieci

15. Jaki jest stopień uzależnienia Państwa działalności od dostępności danych i usług IT:



Wszystkie firmy, które chcą być widoczne w dzisiejszym świecie biznesowym muszą zaakcentować swoją obecność w internecie. Obecność w sieci tworzy także dodatkowe ryzyka, które nie są znane firmom analogowym.

Wśród naszych respondentów prawie 80% firm stwierdziło, że nie jest w stanie prowadzić działalności bez dostępu do danych i usług IT. Około 18% stwierdziło, że brak dostępu do tych danych i usług przez kilka dni byłby bardzo istotnym problemem. Jedynie niecałe 4% respondentów stwierdziło, że przy braku dostępu do ww. usług ich działalność nie byłaby zagrożona, lecz brak możliwości korzystania z nich byłby problemem.

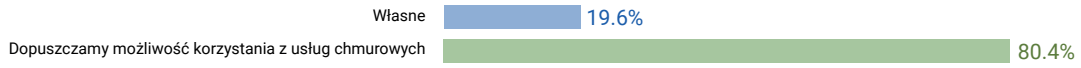
Warto zwrócić uwagę, że żaden z respondentów nie stwierdził, jakoby brak dostępu do danych i usług IT był w stanie łatwo zastąpić w inny sposób.

Wynik odpowiedzi na to pytanie potwierdza jak bardzo ważna jest dostępność danych i usług IT. Ich brak, nawet tylko czasowy, może paraliżować działalność.

Technologie IT stanowią obecnie fundament niemal wszystkich usług, na których przywykliśmy polegać w codziennym życiu. Od bezproblemowej i nieprzerwanej transmisji danych zależą zarówno usługi konsumenckie, a także rozwiązania biznesowe. Każde zakłócenie w dostępności danych może oznaczać różnicę między produktywnością a stratą. Bywa też frustrujące dla użytkowników i wpływa na pogorszenie wizerunku dostawcy usług.

Aktualnie podstawowe działania firm mające na celu zapewnienie dostępności danych sprowadzają się do regularnego tworzenia kopii zapasowych zbiorów danych. W kontekście dzisiejszych potrzeb biznesowych takie działanie jest jednak niewystarczające. Do sprawnego działania biznes potrzebuje bezwarunkowego dostępu do swoich aplikacji i danych, w każdym miejscu i o dowolnej porze. To z kolei wymaga ma wdrożenia odpowiednich rozwiązań organizacyjnych, praktyk biznesowych i narzędzi IT dostosowanych do specyfiki potrzeb biznesowych.

16. Czy Państwa struktura bazuje na własnych systemach czy dopuszczacie Państwo możliwość korzystania z usług chmurowych?



Rozwiązania chmurowe pozwalają firmom na tworzenie kopii zapasowych dowolnych plików, które przechowywane są na serwerze firmy zewnętrznej. Przechowywanie w chmurze pozwala na bezpieczne zapisywanie materiałów w zdalnej bazie danych, dzięki czemu nie trzeba przechowywać swoich danych na dysku komputera lub innym urządzeniu pamięciowym.

Zapewniają one obsługę online na potrzeby przechowywania, udostępniania i synchronizacji plików.

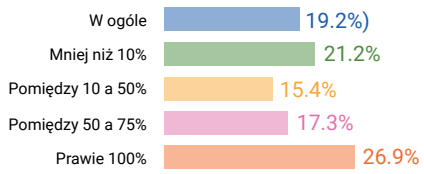
I tak zdecydowana większość naszych respondentów oprócz wykorzystywania własnych dysków twardych dopuszcza możliwość korzystanie z rozwiązań chmurowych (80%). Jedynie niecałe 20% respondentów korzysta wyłącznie z własnych systemów przechowywania danych.

Warto pamiętać, że firmy przechowują dużo wrażliwych danych. Zarówno danych osobowych, jak i danych biznesowych.

Z przechowywaniem danych osobowych w chmurze wiąże się także szereg ryzyk, w tym ryzyko zablokowania lub kradzieży danych przez atak hackerski. Często występują także wątpliwości co do zapewnienia poufności danych. W kontekście przetwarzania danych osobowych, kluczowe będzie także miejsce położenia serwerów, ponieważ, gdy znajdą się one poza terytorium UE, to na gruncie RODO będziemy mieli do czynienia z przekazywaniem danych osobowych do Państw trzecich, co nakłada m.in. na administratora danych osobowych konkretne obowiązki.

Ryzyka te mogą być minimalizowane przez świadomy wybór odpowiedniego i zaufanego partnera dostarczającego rozwiązania chmurowe. W tym celu firmy powinny przeprowadzić właściwą weryfikację dostawcy usług IT, a także zawrzeć umowę zabezpieczającą odpowiednio interesy firmy.

17. Jaka część Państwa sprzedaży realizowana jest poprzez kanały elektroniczne?



Pytanie dotyczące części sprzedaży realizowanej poprzez kanały elektroniczne mogło być problematyczne dla niektórych respondentów. W rozumieniu niniejszego pytania za sprzedaż należy uznać nie tylko stricte e-commerce, w modelu B2C, lecz także sprzedaż prowadzoną w modelu B2B za pośrednictwem wiadomości e-mail czy też innych kanałów komunikacji elektronicznej.

Blisko 30% respondentów wskazała, że prawie 100% ich sprzedaży realizowana jest poprzez kanały elektroniczne. W ogóle sprzedaży poprzez kanały elektroniczne nie prowadziło jedynie ok. 20% respondentów. Pozostała część w większym lub mniejszym zakresie prowadziła sprzedaż przez internet, a w pozostałej części prowadziła sprzedaż tradycyjnymi kanałami sprzedażowymi (sklepy stacjonarne, targi, itp.).

Podsumowanie rozdziału III.

- Blisko 80% badanych firm stwierdziło, że nie jest w stanie prowadzić działalności bez dostępu do danych i usług IT. Około 18% stwierdziło, że brak dostępu do tych danych i usług przez kilka dni byłby bardzo istotnym problemem. Jedynie niecałe 4% respondentów stwierdziło, że przy braku dostępu do ww. usług ich działalność nie byłaby zagrożona, lecz brak możliwości korzystania z nich byłby problemem.

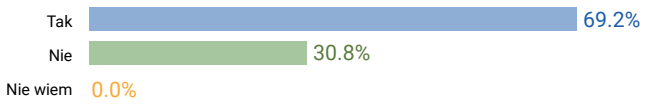
- Wynik ten potwierdza jak bardzo ważna jest dostępność danych i usług IT. Ich brak, nawet tylko czasowy, może paraliżować działalność biznesową.

- Zdecydowana większość respondentów oprócz wykorzystywania własnych dysków twardych dopuszcza możliwość korzystanie z rozwiązań chmurowych (80%). Jedynie niecałe 20% respondentów korzysta wyłącznie z własnych systemów przechowywania danych.

- Blisko 30% respondentów wskazało, że prawie 100% ich sprzedaży realizowana jest poprzez kanały elektroniczne. W ogóle sprzedaży poprzez kanały elektroniczne nie prowadziło jedynie ok. 20% respondentów. Pozostała część w większym lub mniejszym zakresie prowadziła sprzedaż przez internet.

IV. Doświadczenie z cyberatakami. Pracownicy. Edukacja

18. Czy Państwa firma odnotowała w 2021 roku incydenty dotyczące cyberbezpieczeństwa Państwa systemów?

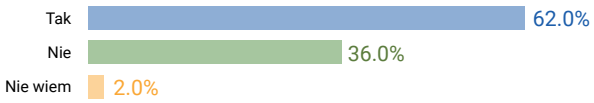


70% badanych firm odnotowało incydenty z zakresu cyberbezpieczeństwa. 30% respondentów incydentów takich nie odnotowało, co jednak nie oznacza, że nie były one przedmiotem ataków. Średni czas na wykrycie incydentów według raportu IBM wykrycie oraz zlikwidowanie5 incydentu w zakresie cyberbezpieczeństwa zajmuje średnio 287 dni. Nie wykluczone zatem, że do wielu incydentów, o których mówili respondenci doszło w roku 2020. Równie możliwe jest także to, że wiele z firm udzielających negatywnych odpowiedzi, nie ma świadomości ataku dokonanego na ich infrastrukturę IT.

Niezależnie od tych wątpliwości, wydaje się, że od 2018 roku, tj. od daty uchwalenia UKSC znacznie wzrosła świadomość firm w odniesieniu do tego czym w istocie jest incydent w zakresie cyberbezpieczeństwa.

5 *"IBM Cost of a Data Breach Report 2021" dostęp z dnia 04.04.2022 r. https://www.ibm.com/downloads/cas/OJDVQGRY*

19. Czy kiedykolwiek zgłosili Państwo zawiadomienie o podejrzeniu popełnienia przestępstwa w związku z wystąpieniem incydentu?



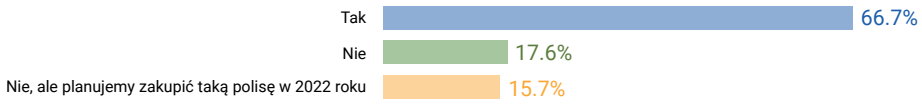
Kodeks karny zawiera dość rozbudowaną taksonomię przestępstw przeciw ochronie informacji, choć ściganie takich przestępstw jest niezmiernie trudne z uwagi na globalny charakter działalności przestępczej w tym zakresie oraz trudność w uzyskiwaniu i zabezpieczaniu dowodów w krajach trzecich, w szczególności w sytuacjach w których działalność przestępcza jest bardzo często pośrednio lub bezpośrednio wspierana przez państwo. Wysoki odsetek dokonanych zgłoszeń tj. 62% wobec 70% przypadku wystąpienia incydentu, wskazuje na rosnącą świadomość istnienia prawnych środków ochrony, choć jeżeli chodzi statystyki policyjne, to wydają się one rozmijać z takim wnioskiem.

Przykładowo, jeżeli chodzi o przestępstwo z art. 269a Kodeksu Karnego6 (tzw. sabotaż komputerowy), to statystyki policyjne odnotowały w roku 2020… 30 zgłoszeń w tym zakresie 7, z czego jedynie w 20 przypadkach potwierdzono fakt popełnienia przestępstwa.

6 *„Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5."*

7 *Strona www.statystyka.policja.pl - dostęp z dnia 04.04.2022 r. https://statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-14/63630,Sabotaz-komputerowy-art-269a.html*

20. Czy korzystają Państwo z polisy na wypadek wystąpienia cyberzagrożenia?



Pytanie dotyczące korzystania przez firmy z polisy ubezpieczeniowej na wypadek wystąpienia cyberataku początkowo wywoływało wśród respondentów konsternację. Zaobserwowaliśmy, że ubezpieczenia na wypadek wystąpienia cyberataków nie są w Polsce popularne, a na pewno nie są tak powszechne, jak na zachodzie, a w szczególności w USA.

Najczęściej jednak respondenci (66%) odpowiadali, że ich firma jest objęta ubezpieczeniem na wypadek start poniesionych w drodze cyberataku. W dużej części respondenci podkreślali, że ubezpieczenie to nie jest jednak dodatkową polisą, a ubezpieczenie na wypadek szkód poniesionych w drodze cyberataków obejmuje ich główna polisa ubezpieczeniowa dotycząca podstawowej działalności firmy. Tylko 1/3 respondentów wskazała, że nie korzysta aktualnie z tego rodzaju polisy ubezpieczeniowej, lecz prawie 50% z respondentów odpowiadających negatywnie na to pytanie stwierdziło, że zamierza bliżej przyjrzeć się tematowi w nadchodzących tygodniach i planuje nabyć przedmiotową polisę w 2022 roku.

Aktualnie możemy zaobserwować zwiększoną liczbę zdarzeń cybernetycznych, wynikających nie tylko z wojny na Ukrainie, lecz także z powodu przeniesienia większości biznesowego i codziennego życia do cyberprzestrzeni na skutek pandemii COVID-19.

Agencja ratingowa Fitch twierdzi, że w 2020 roku tylko w samych Stanach Zjednoczonych koszty ubezpieczeń cyber wyniosły ponad 2,7 miliarda dolarów, co obejmuje działalność związaną z naprawą zhackowanych sieci, stratami związanymi z przerwami w prowadzeniu działalności, a także płaceniem okupu8.

Ubezpieczenia odnoszące się wyłącznie do cyberataków nie są oczywiście rozwiązaniami tanimi.
Stawki ubezpieczeń cybernetycznych wzrosły o 130 proc. w USA i o 92 proc. w Wielkiej Brytanii w czwartym kwartale ub.r. Podobne wzrosty mają być prognozowane na ten rok. „Ceny wszystkich wzrosły, teraz wzrosną jeszcze bardziej" – stwierdzili eksperci, wskazując jako przyczynę wojnę ukraińsko-rosyjską9.

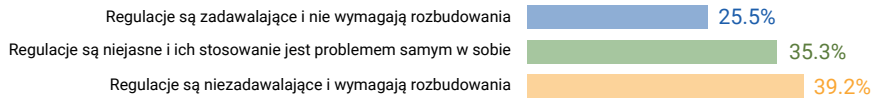
Przy wyborze odpowiedniej polisy ubezpieczeniowej warto zwrócić uwagę na wszelkie szczegółowe postanowienia Ogólnych Warunków Umowy Ubezpieczenia w zakresie wyłączeń odpowiedzialności ubezpieczyciela.

8 https://cyberdefence24.pl/cyberbezpieczenstwo/ubezpieczenie-na-wypadek-cyberatakow-wojna-w-ukrainie-i-roszczenia-o-odszkodowania *dostęp z dnia 04.04.2022 r.*
9 *Ibidem.*

21. Czy planują Państwo zwiększyć w 2022 nakłady inwestycyjne związane z cyberbezpieczeństwem?

Pomimo faktu, że 40% respondentów nie posiada wyodrębnionego budżetu na wydatki w zakresie cyberbezpieczeństwa, aż 90% respondentów spodziewa się zwiększenia nakładów inwestycyjnych w tym obszarze w roku 2022. Jest to zrozumiałe o tyle, że w zasadzie nie ma tygodnia bez nowych informacji dotyczących kolejnych problemów związanych z atakami hackerskimi. Ich liczba, pomysłowość a także szkodliwość wydaje się rosnąć proporcjonalnie do tempa rozwoju transformacji cyfrowej w poszczególnych obszarach gospodarki. Liczba firm których działalność może zostać całkowicie zatrzymana na skutek ataku na ich infrastrukturę cyfrową wzrasta każdego dnia. Inną kwestią są wymogi regulacyjne i to nie tylko te związane z UKSC czy też regulacjami branżowymi, ale także – a być może przede wszystkim te – związane z ochroną danych osobowych. W Polsce mamy już kilka przypadków kar nałożonych przez regulatora w związku z naruszeniem przepisów RODO dotyczących ochrony tych danych, związanych bezpośrednio lub pośrednio z atakami hackerskimi których ofiarami padali administratorzy takich danych.

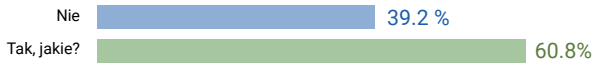
22. Jak oceniacie Państwo stan regulacji prawnych w zakresie cyberbezpieczeństwa?



Z odpowiedzi udzielonych w Raporcie na temat stanu regulacji prawnych wynika, że źródła obowiązków prawnych co do spraw cyberbezpieczeństwa są niezwykle rozgałęzione. Pochodzą one także z aktów prawnych na różnym poziomie. Czasami z dyrektyw, które kolejno implementowane są do porządków krajowych z pewnymi różnicami. Przejrzystości wymagań nie sprzyja także coraz to bogatszy zbiór dokumentów wydawanych przez organy nadzoru. W tych samych sprawach, np. ryzyka ICT, outsourcingu czy korzystania z usług chmurowych wytyczne pochodzą od różnych organów, tak na poziomie krajowym, jak i wspólnotowym (UE). Takiemu rozproszeniu systemu, przynajmniej dla sektora finansowego, zapobiegać ma wspomniane rozporządzenie DORA, które podobnie jak RODO będzie obowiązywało w państwach członkowskich UE bezpośrednio.

Taki stan rzeczy odpowiada wynikom badań naszego Raportu, wedle których: 36% badanych uznaje regulacje w zakresie cyberbezpeczeństwa za niejasne, i co więcej, że ich stosowanie jest problemem samym w sobie; 40% uznało, że regulacje są niezadawalające i wymagają rozbudowana. Przenosząc to na zarysowane powyżej problemy, być może należałoby jeszcze wskazać, że wymagają one ujednolicenia. 25% respondentów wskazało zaś, że regulacje są zadawalające i nie wymagają rozbudowania.

23. Czy wprowadzili Państwo u siebie odrębne zasady mające na celu weryfikowanie zakupów dokonywanych przez firmę oraz kontraktów zawieranych przez firmę pod kątem cyberbezpieczeństwa?



Niepokojący wydaje się wynik odpowiedzi na pytania o procesy zakupowe, gdzie tylko 61% naszych respondentów wskazało, że posiada odrębne zasady mające na celu weryfikowanie zakupów dokonywanych przez firmę oraz kontraktów zawieranych przez firmę pod kątem cyberbezpieczeństwa. Jest to niewątpliwie proces, który wymaga więcej uwagi, a odpowiednie regulacje wewnętrzne mogą przyczynić się do zarządzenia ryzykiem ICT przy wprowadzeniu nowych rozwiązań u danego przedsiębiorcy na samym początku. Mogą również przyczynić się do wyeliminowania dostawcy, który nie spełnia wymagań z zakresu privacy by design czy secure by default. To w naszej ocenie sfera, która wymaga wyraźnej poprawy w zarządzaniu cyberbezpieczeństwem u przedsiębiorców w ramach dobrych praktyk w każdym sektorze. W sektorze finansowym najpewniej takie rozwiązania (o ile już nie zostały) zostaną wdrożone powszechnie wskutek rozporządzenia DORA, które wspomina o; [1] wzorze rejestru postanowień umownych, [2] wytycznych audytowych, czy [3] politykach i procedurach nadzoru dostawcy. Nie sposób bowiem sobie wyobrazić sprawowania kontroli nad zakresem czynności powierzonych dostawcy, ochrony przed vendor-lockiem i mitygowaniem ryzyka cyberbezpieczeństwa, gdy dostawca nie zostanie zweryfikowany już na etapie ofertowania.

Powyższe koresponduje również z funkcjonującymi już w obrocie wytycznymi organów nadzoru i tak, np. wytyczne EIOPA (Europejski Urząd Nadzoru Ubezpieczeń) w sprawie zarządzania ryzykiem ICT10 czy wytyczne EBA w sprawie zarządzania ryzykiem związanym z technologiami i bezpieczeństwem ICT11.

Trendy w zarządzaniu cyberbezpieczeństwem, a także świadomość regulacji prawnych oraz wspominanych wytycznych o charakterze softlaw, które organy wprowadzają do swoich praktyk nadzorczych, znajdują odzwierciedlenie w poziomie świadomości organizacji. Ta świadomość nie jest naturalnie tak wysoka, jak ta, która wynika z powszechnie obowiązujących przepisów, jak chociażby RODO12. W przypadku tego rozporządzenia, z uwagi na jego powszechne obowiązywanie, możemy stwierdzić, że procedury zostały wdrożone przez niemal każdego przedsiębiorcę, który przetwarza dane osobowe (niezależnie od tego czy w swoim imieniu czy na zlecenie innego administratora danych). Z takiego stanu rzeczy jasno wynika, że regulacje prawne oraz związania z nimi kontrola sankcje stanowią czynnik motywujący dla zaadresowania określonych ryzyk w działalności biznesu.

10 https://www.eiopa.europa.eu/document-library/guidelines/guidelines-information-and-communication-technology-security-and_en
11 https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management
12 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

We wspomnianych wytycznych organów nadzoru znaczenie nadaje się również poziomowi świadomości w zakresie cyberbezpeczeństwa. I co istotne, organy wskazują, że świadomość organizacji zależy od świadomości każdego z jej członków. Stąd bierze się postulat okresowych szkoleń z tego zakresu oraz uwzględnienia cyberbezpiezceństwa z punktu widzenia zarządzania ryzykiem ICT w przedsiębiorstwach. W niektórych wytycznych niejako w odpowiedzi na problemy zgłaszane przez rynek wysuwa się postulat wprost do zarządu, z którego wynika potrzeba zabezpieczenia budżetu na zwiększania świadomości pracowników z zakresu cyberbezpieczeństwa.

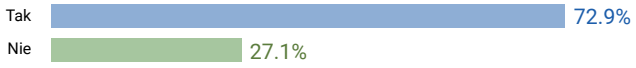
24. Czy w Państwa firmie wykonywane są jednorazowe testy związane z cyberbezpieczeństwem wprowadzanych nowych usług lub produktów?

25. Czy w Państwa firmie wykonywane są okresowe testy związane z cyberbezpieczeństwem, np. pentesty?

Wpływ zmieniającej się rzeczywistości biznesu i ryzyk związanych ze sferą cyber znajduje odzwierciedlenie w wynikach naszego Raportu, wedle których 86,5% przedsiębiorców wykonuje jednorazowe testy bezpieczeństwa dla nowych usług lub produktów. Co więcej, 92,3% respondentów podało, że w ich organizacjach wykonuje się okresowe testy związane z cyberbezpieczeństwem. To pytanie dość ogólne, ale pomimo to pokazuje pozytywny obraz, że przedsiębiorcy spoglądają już na kwestię cyberbezpieczeństwa jako proces. Nie testują bowiem jedynie na początku i jednorazowo, a traktują tę sprawę jako stały element zarządzania ryzykiem ICT.

26. Czy Państwa organizacja szkoli pracowników z zakresu cyberbezpieczeństwa?

27. Czy szkoleniami objęci są wszyscy pracownicy?



28. Czy są to szkolenia obowiązkowe?

Zapobieganie jest zawsze lepszym rozwiązaniem niż leczenie. To rozwiązanie znane jest już od bardzo dawna.

Także zapobiegliwe firmy, które preferują prewencję przed cyberatakami, mogą zapobiegać wystąpieniu negatywnych konsekwencji w zakresie wirtualnych zagrożeń.

W jaki sposób? Jedną z form zapobiegania mogą być szkolenia pracowników, co jak wskazaliśmy we wcześniejszej części Raportu, jest rekomendowane przez organy nadzoru, celem zadbania o odpowiedni poziom świadomości w zakresie cyberbezpieczeństwa.

Aż 85% respondentów wskazało, że przeprowadza szkolenia z zakresu cyberbezpieczeństwa. Szkolenia w firmach, z którymi przeprowadziliśmy wywiad polegały w głównej mierze na szkoleniach, w których prowadzący opowiadał o występujących zagrożeniach i sposobach walki z nimi lub na e-learningach zakończonych testem. Bardzo często szkolenia są okresowe (raz na kwartał, raz do roku) i kończą się sprawdzeniem wiedzy pracownika. W przypadku, gdy nie przekroczy on progu zdawalności, musi odbyć szkolenie ponownie. Bardziej świadomi pracownicy preferowali przeprowadzenie egzaminu potwierdzającego świadomość cyberzagrożeń bez odbycia szkoleń.

Duża część firm stwierdzała także, że oprócz szkoleń przeprowadzanych okresowo, organizuje szkolenia w przypadku zaistnienia incydentu.

Wyłącznie ok. 15% badanych firm nie przeprowadzało szkoleń z omawianego zakresu. Niemniej, brak szkoleń nie wynikał z braku przewidywania zagrożeń lub też zbyt niskich budżetów szkoleniowych, a z tego, że firmy mają pewność co do świadomości swoich pracowników. Pracownicy natomiast potwierdzali swoją świadomość niezwłocznie zgłaszając firmie wszelkie niepokojące sygnały mogące świadczyć o występującym cyber-

zagrożeniu.
Trzy czwarte ankietowanych firm obejmowało przedmiotowymi szkoleniami wszystkich pracowników. Pozostała część respondentów albo nie przeprowadzała szkoleń w ogóle (8 firm zgodnie z odpowiedziami na pytanie nr. 26) lub przeprowadzała szkolenia wyłącznie w odniesieniu do wybranych grup pracowników.

Co naturalne, w dużej mierze szkoleniami nie byli objęci pracownicy, którzy na co dzień nie mają do czynienia z pracą z wykorzystaniem dostępu do danych firmowych zawartych na serwerach firmy i w chmurze.

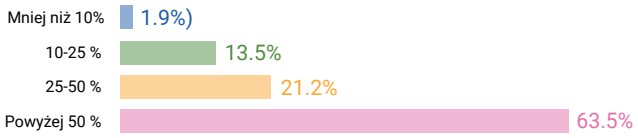
Firmy, które objęły szkoleniami wszystkich pracowników, wprowadziły także wymóg obowiązkowego udziału w nich. Tego rodzaju podejście jest w pełni uzasadnione. Jeżeli chcemy odpowiednio zabezpieczyć firmę, to pracownicy muszą być świadomi czyhających na nich zagrożeń.

Należy pamiętać, że nauka pracowników o zagrożeniach nie kończy się na szkoleniach czy e-learningach. Respondenci podkreślali, że prowadzą także kontrolowane ataki phishingowe oraz inne formy cyberataków. W taki sposób w praktyce mogą sprawdzić, jak reagują ich pracownicy na ataki, które w normalnych okolicznościach przeprowadzone byłyby przez przestępców pragnących uzyskać dostęp do danych firmy.

Aby zapewnić skuteczność kontrolowanych ataków, są one przeprowadzane przez zewnętrzne firmy lub przez ograniczone grono pracowników działu cyberbezpieczeństwa lub IT firmy.

Oczywiście, tak jak stwierdził jeden z naszych respondentów „firmy dzielą się na te które były, są lub będą zhackowane", lecz im wyższa świadomość zagrożeń wśród pracowników, tym mniejsze ryzyko zbyt łatwego zhackowania firmy.

29. Ilu pracowników Państwa firmy korzysta z pracy zdalnej w wymiarze przynajmniej 1 dnia tygodniowo?



Rok 2021 dla wielu przebiegał pod hasłem transformacji cyfrowej. Niekiedy mniej a innym razem bardziej przymuszonej. Jednym z wyzwań było wdrożenie pracy zdalnej. Więcej o pracy zdalnej pisaliśmy w 2020 r. w raporcie DGTL – HR COMPLIANCE – dostępnym na www.dgtl.law w zakładce publikacje pod tytułem: Raport o pracy zdalnej. Powszechne wręcz zainteresowanie pracą zdalną w ubiegłym roku potwierdzają także dane KPMG podane w raporcie – Barometr Cyberbezpieczeństwa – aż 83% polskich firm wdrożyło pracę zdalną w 2021. Firmy obok wyzwań prawnych, równolegle mierzyły się z kwestiami technologicznymi. Te drugie rozwiązywane były, np. przez wdrożenie szyfrowanych połączeń za pomocą VPN[13]. Jednocześnie to kolejny dowód, że w środowisku cyfrowym współpraca prawników z pracownikami bezpieczeństwa stała się niezbędna.

Praca zdalna aktualnie jest naszą codziennością.

Korzystanie z pracy zdalnej zwiększa ryzyko zhackowania pracownika poprzez uzyskanie dostępu do jego sieci domowej (zazwyczaj gorzej zabezpieczonej niż sieć firmy) lub też zmniejszoną czujność pracownika spowodowaną przebywaniem w otoczeniu domowym.

Prawie wszyscy respondenci zezwalają swoim pracownikom na korzystanie z pracy zdalnej w wymiarze co najmniej 1 dnia tygodniowo. Tylko 1 respondent wskazał, że z uwagi na charakter swojej działalności tylko pracownicy biurowi, stanowiący do 10% ogółu pracowników, są upoważnieni do wykonywania pracy zdalnej w wymiarze co najmniej 1 dnia tygodniowo.

Udzielając pracownikom prawa do wykonywania pracy w formie zdalnej warto zadbać o bezpieczeństwo firmy. Bezpieczeństwo to będzie zwiększone, gdy pracownik będzie odpowiednio przeszkolony z zakresu bezpieczeństwa w pracy zdalnej. Kluczowe w tym zakresie może być przypomnienie pracownikowi, aby nie logował się do publicznego Wi-Fi, nie udostępniał sprzętu służbowego członkom swojej rodziny (ani innym nieupoważnionym osobom) oraz nie korzystał ze służbowej skrzynki mailowej do prywatnej korespondencji.

Odpowiednie poinformowanie pracowników o zasadach pracy zdalnej, w tym zasadach cyberbezpieczeństwa, może nastąpić w procedurze pracy zdalnej, która powinna odnosić się także do kwestii cyberbezpiecznej pracy zdalnej.

13 *Wirtualna sieć prywatna, która szyfruje dane w czasie przesyłania (virtual private network)*

Podsumowanie rozdziału IV.

- 70% badanych firm odnotowało incydenty z zakresu cyberbezpieczeństwa. 30% respondentów incydentów takich nie odnotowało, co jednak nie oznacza, że nie były one przedmiotem ataków. Możliwe jest, że wiele z firm udzielających negatywnych odpowiedzi, nie ma świadomości ataku dokonanego na ich infrastrukturę IT.

- Wydaje się, że od 2018 roku, tj. od daty uchwalenia UKSC znacznie wzrosła świadomość firm w odniesieniu do tego czym w istocie jest incydent w zakresie cyberbezpieczeństwa.

- Wysoki odsetek dokonanych zawiadomień o podejrzeniu popełnienia przestępstwa w przypadku wystąpienia cyberincydentu, wskazuje na rosnącą świadomość istnienia prawnych środków ochrony, choć jeżeli chodzi statystyki policyjne, to wydają się one rozmijać z takim wnioskiem.

- Najczęściej respondenci (66%) odpowiadali, że ich firma jest objęta ubezpieczeniem na wypadek start poniesionych w drodze cyberataku. W dużej części respondenci podkreślali, że ubezpieczenie to nie jest jednak dodatkową polisą, a ubezpieczenie na wypadek szkód poniesionych w drodze cyberataków obejmuje ich główna polisa ubezpieczeniowa dotycząca podstawowej działalności firmy.

- Aż 90% respondentów spodziewa się zwiększenia nakładów inwestycyjnych w tym obszarze w roku 2022.

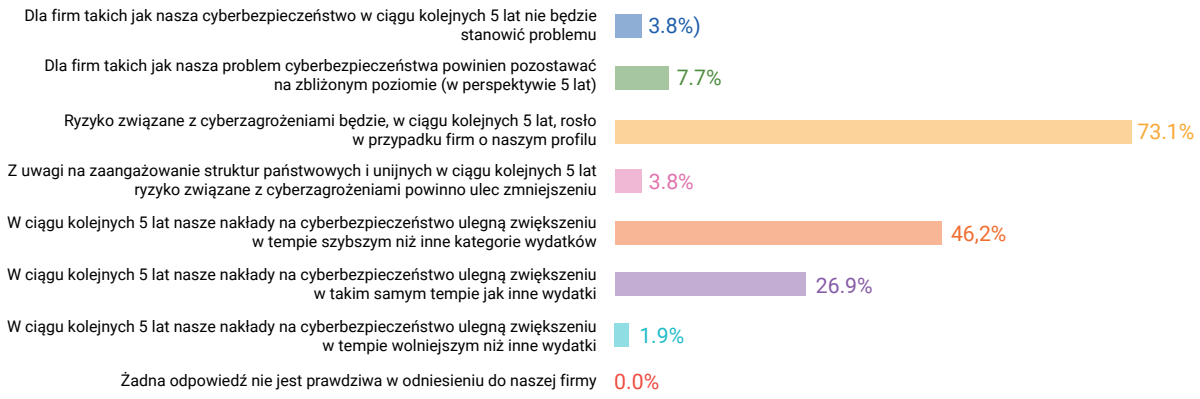
- Tylko 61% naszych respondentów wskazało, że posiada odrębne zasady mające na celu weryfikowanie zakupów dokonywanych przez firmę oraz kontraktów zawieranych przez firmę pod kątem cyberbezpieczeństwa.

- 86,5% przedsiębiorców wykonuje jednorazowe testy bezpieczeństwa dla nowych usług lub produktów. Co więcej, 92,3% respondentów podało, że w ich organizacjach wykonuje się okresowe testy związane z cyberbezpieczeństwem.

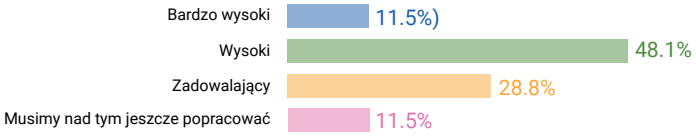
- Aż 85% respondentów wskazało, że przeprowadza szkolenia z zakresu cyberbezpieczeństwa. Szkolenia w firmach, z którymi przeprowadziliśmy wywiad polegały w głównej mierze na szkoleniach, w których prowadzący opowiadał o występujących zagrożeniach i sposobach walki z nimi lub na e-learningach zakończonych testem. Bardzo często szkolenia są okresowe (raz na kwartał, raz do roku) i kończą się sprawdzeniem wiedzy pracownika.

V. Przyszłość

30. Proszę zaznaczyć zdanie lub zdania które są prawdziwe w odniesieniu do Państwa firmy:



31. Jak oceniłby/łaby Pan/i stopień przygotowania Państwa organizacji na incydenty cyberbezpieczeństwa?



W kontekście świadomości cyberzagrożeń należy pozytywnie odnieść się do świadomości naszych respondentów. 73% naszych respondentów wskazało, że ryzyko związane z cyberzagrożeniami będzie w ciągu kolejnych 5 lat rosło w przypadku firm o ich profilu.

Dostarczającą wartościowej informacji jest również odpowiedź, iż 46,2% respondentów, którzy wskazali, że w ciągu kolejnych 5 lat nakłady ich organizacji na cyberbezpieczeństwo ulegną zwiększeniu w tempie szybszym niż inne kategorie wydatków. Odpowiedź niemalże połowy respondentów jest zgodna z trendem globalnym, wedle którego do 2026 wydatki na cyber wzrosną do 16,8 miliardów dolarów amerykańskich[14].

Jako pozytywny symptom należy także określić odpowiedź ankietowanych w naszym Raporcie na pytanie dotyczące oceny stopnia przygotowania organizacji badanego na incydenty cyberbezpieczeństwa. Tylko 11,5% oceniło ten stopień na bardzo wysoki, z czego można wnioskować, że przedsiębiorcy świadomi są powagi wyzwania, a także najprawdopodobniej tego, że jest to proces wymagający stałego doskonalenia.

14 *Connected and Protected: The Vulnerabilities and Opportunities of IoT Security za Raportem: Cyberbezpieczeństwo w Polsce 2021 r., cyberataki na urządzenia końcowe, Cyfrowa Polska*

Podsumowanie rozdziału V.

- Aż 73% respondentów wskazało, że ryzyko związane z cyberzagrożeniami będzie w ciągu kolejnych 5 lat rosło w przypadku firm o ich profilu.

- 46,2% respondentów, którzy wskazali, że w ciągu kolejnych 5 lat nakłady ich organizacji na cyberbezpieczeństwo ulegną zwiększeniu w tempie szybszym niż inne kategorie wydatków. Odpowiedź niemalże połowy respondentów jest zgodna z trendem globalnym, wedle którego do 2026 wydatki na cyber wzrosną do 16,8 miliardów dolarów amerykańskich[15].

- Tylko 11,5% respondentów oceniło stopień przygotowania incydenty na bardzo wysoki, z czego można wnioskować, że przedsiębiorcy świadomi są powagi wyzwania, a także najprawdopodobniej tego, że jest to proces wymagający stałego doskonalenia.

15 Connected and Protected: The Vulnerabilities and Opportunities of IoT Security za Raportem: Cyberbezpieczeństwo w Polsce 2021 r., cyberataki na urządzenia końcowe, Cyfrowa Polska

Złote cytaty respondentów:

„Największym problemem z jakim będą musiały się mierzyć osoby odpowiedzialne za cyberbezpieczeństwo będą braki w zasobach ludzkich. Problemem nie będzie brak technologii czy sprzętu, lecz brak odpowiednio wykwalifikowanych specjalistów z obszaru cyber. W Polsce już teraz mamy bardzo dużo firm, które korzystają ze specjalistów z zakresu cyber, których jest ciągły brak. Będzie on w najbliższym czasie będzie jeszcze bardziej widoczny. Firma będzie musiała zadowolić pracowników, bo w przeciwnym wypadku odejdą całe zespoły."

„Dobry Security Manager to dietetyk ryzyka"

„Być dyrektorem wiedzy, a nie mówienia nie" (know/no)

"Security Managerowie muszą mieć wpływ na biznes"

„Na IT wydajemy za mało!!!"

„Jako branża mamy duży dług technologiczny do spłacenia"

„Zgodność zaczyna przeszkadzać w prowadzeniu biznesu"

„Organizacje dzieli się na te, które były, są lub będą zhackowane"

„Gotowość na ataki jest konieczna i poprawne cyberbezpieczeństwo też jest konieczne"

„Największym wyzwaniem najbliższych lat będą bardzo szybko zmieniające się regulacje, które są niejasne"

„Dużym wyzwaniem będzie wojna na Ukrainie i wypływające z niej zagrożenia cyberwojną"

„Żadne prawo nie zabezpieczy przed atakami"

„Nie klikaj! Zapytaj!" – w kontekście dziwnych linków i maili

„Nie trzymamy haseł na karteczkach"

„Niezbędna jest zmiana mentalności ludzi, aby podchodzili do swoich obowiązków w sposób dojrzały, ponieważ nawet bardzo wysoko zabezpieczone sprzęty i dane, są narażone na zhackowanie na skutek błędu ludzkiego."

NIS - reaktywacja

Kiedy cztery lata temu pojawiła się dyrektywa 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dalej „Dyrektywa NIS"), wydawało się, że zostanie z nami na dłużej. Adresowała przecież obszar, który nie był do tego momentu przedmiotem żadnej spójnej regulacji, a wiadomym było, że w niektórych krajach (między innymi w Polsce), jej implementacja oznacza stworzenie zupełnie nowej dziedziny prawa.

To zaś nie dzieje się z dnia na dzień. Większość krajów faktycznie uchwaliła przepisy implementujące Dyrektywę NIS do prawa krajowego w zakładanym terminie, czyli do 10 maja 2018 r. Jeżeli chodzi jednak o proces wdrożenia tych postanowień, to tu zaczęły się schody. W Polsce, która zaimplementowała bardzo rozbudowany model administracji obszarem cyberbezpieczeństwa, praktycznie do czasów obecnych nie wydano jeszcze wszystkich decyzji o wyznaczeniu operatorów usług krytycznych. Warto wspomnieć, że nie przeszkodziło to nam dopracować się ostatnio projektu zmiany tej ustawy, który ten układ dodatkowo skomplikuje. Jak jednak widać, zakusy wprowadzania ulepszeń do regulacji nie są wyłącznie naszą specjalnością. Komisja Europejska analizując obecny stan systemu regulacji w zakresie cyberbezpieczeństwa, doszła do wniosku, że zmiany są niezbędne. I to zmiany w takim zakresie, że konieczne będzie uchwalenie zupełnie nowej dyrektywy. Tu i ówdzie pojawiały się nawet poglądy, że może tak wzorem RODO warto byłoby się pokusić o rozporządzenie, ale pomysł ten nigdy się nie skrystalizował. Należy pamiętać, że rozporządzenie w sprawie ochrony danych osobowych, było wprowadzone po kilkunastu latach obowiązywania poprzedzającej je dyrektywy, która obowiązując wiele lat, na dobre zadomowiła się w systemach państw członkowskich. Było na czym budować. W przypadku Dyrektywy NIS nie ma mowy o porównywalnym doświadczeniu, stąd w propozycji jedynie zmiana treści, ale nie rodzaju aktu prawnego. Dlaczego zmian okazała się konieczna?

Wiele elementów nie działa. Jak działają, to na ogół źle, a jeśli działają dobrze - to nie przynoszą oczekiwanych rezultatów

Zdaniem KE Dyrektywa NIS I objęła zbyt wąską grupę przedsiębiorstw, a to z uwagi na to, że stopień usieciowienia i cyfryzacji przekroczył znacznie zakładane wcześniej wielkości. Skutkiem czego pojawiły się obszary kluczowe dla rozwoju cyfrowej gospodarki europejskiej, pozostające poza zasięgiem oddziaływania dyrektywy. Gdyby był to jedyny problem, wystarczyłaby zapewne korekta obecnie obowiązującej dyrektyw. Ale tak nie jest. Zdaniem Komisji, rozwiązaniom przyjętym w NIS I brakowało wystarczającej precyzji, skutkiem czego określone grupy przedsiębiorstw były regulowane w kilku krajach, a w kilku innych już nie (przykładowo szpitale). Rozjechały się także systemy raportowania przyjmowane przez poszczególne państwa europejskie, co utrudniało, a czasami uniemożliwiało efektywne zarządzenie wyzwaniem cyberzagrożeń w skali europejskiej. Do tego doszedł nieefektywny nadzór i brak odpowiednio sprawnej egzekucji, olbrzymie zróżnicowanie w nakładach na zasoby ludzkie i budżetowe przypisane do realizacji zadań opisanych w NIS I i brak systematycznego współdzielenia informacji pomiędzy państwami UE. Patrząc na wyliczankę Komisji, aż chciałoby się zapytać: to co w końcu zadziałało? Faktycznie.

W mieście pojawi się nowy szeryf… z licencją na zamykanie

Czytając projekt NIS II widać zupełnie inne podejście do niektórych kwestii. I może warto zacząć od końca. Wszyscy recenzenci Dyrektywy NIS I, byli zgodni, że w kwestiach egzekucji naruszeń i sankcji z tym związanych, dyrektywa ta była niezwykle lakoniczna. Skutek, był taki, że w Polsce najwyższą możliwą karą do nałożenia za naruszenie ustawy była kara jednego mln złotych. Biorąc pod uwagę fakt, że polska ustawa o krajowym systemie bezpieczeństwa wchodziła w życie mniej więcej w tym samym czasie, kiedy przedsiębiorcy mierzyli się z wyzwaniami RODO oraz drakońskimi karami przewidzianymi w tym rozporządzeniu, niewielu było takich, którzy wierzyli w możliwość sprawnego wdrożenia ustawy pozbawionej realnych sankcji. Według projektu NIS II, element ten ulegnie diametralnej zmianie. I to nie dlatego, że maximum kary wzrośnie do 10 mln Euro (czyli prawie czterdzieści pięć razy), albo 2% łącznego rocznego obrotu uzyskanego na całym świecie, ale dlatego, że zgodnie z projektem nowej dyrektywy państwa członkowskie będą musiały wprowadzić szereg mechanizmów zwiększających prawdopodobieństwo przestrzegania nowych przepisów. Czego zatem mogą spodziewać się przedsiębiorcy podlegający nowym przepisom po implementacji NIS II? Inspekcji w swojej siedzibie, nadzoru nad działaniami prowadzonymi on-line, losowych weryfikacji. Oprócz obowiązków przeprowadzania standardowych audytów pojawią się audyty celowe związane z oceną ryzyka. Konieczność dostarczania określonej dokumentacji na życzenie uprawnionych organów. Konieczność udzielania dostępu do danych, jeśli jest to konieczne dla sprawowania nadzoru. Krajowe organy nadzoru mają zostać wyposażone w uprawnienia, które wskazują na to, że w Polsce pojawi się kolejny obok UOKiK, UKE oraz UODO organ posiadający bardzo daleko idące uprawnienia. Ostrzeżenie jest najłagodniejszym z nich. Kolejnym jest wiążąca instrukcja lub nakaz dotyczący usunięcia zidentyfikowanych niezgodności lub naruszeń obowiązków przewidzianych w NIS II. Nakaz podjęcia określonych działań w zakresie zarządzania ryzykiem - w określony sposób i w określonym czasie. Nakaz poinformowania osób, na rzecz których przedsiębiorca świadczy usługi o grożącym im zagrożeniu i istniejących możliwościach podjęcia przez takie osoby konkretnych działań mających na celu zaadresowanie tych ryzyk. Nakaz wdrożenia zaleceń audytu w określonym terminie. Regulator będzie też mógł delegować swojego pracownika do nadzorowania (w określonym czasie) wskazanych działań w zakresie wprowadzania obowiązków przewidzianych w NIS II oraz podawać do publicznej wiadomości nazwy przedsiębiorców, którzy dopuścili się naruszeń Dyrektywy oraz rodzaju tych naruszeń. A także … a jakże, nakładać kary. Do tego dochodzi możliwość zawieszenia autoryzacji lub certyfikacji określonych usług i zawieszania w obowiązkach osób z kierownictwa firmy dopuszczającej się naruszeń.

Kluczowe, Ważne i … Małe też

NIS II utrzyma kategorię operatorów usług krytycznych, ale znika kategoria dostawców cyfrowych, których obowiązki w NIS I kształtowane były nieco odmiennie. Zamiast dostawców usług cyfrowych pojawi się druga kategoria operatorów usług istotnych, w skład której wejdą m. in.: firmy pocztowe i kurierskie, firmy składujące i przetwarzające odpady, wytwórcy, producenci oraz dystrybutorzy chemikaliów, producenci i dystrybutorzy żywności, producenci przemysłowi oraz dostawcy cyfrowi). Mikro oraz mali przedsiębiorcy (przedsiębiorcy zatrudniający do 50 osób, których roczny bilans nie przekracza 10 mln Euro), będą z ustawy wyłączeni, chyba, że stosować się będzie do nich jeden z wyjątków opisanych w NIS II. Przykładowo tacy, w przypadku których naruszenie świadczonych przez nich usług mogłoby mieć wpływ na bezpieczeństwo publiczne, albo zdrowie publiczne. Dość pojemny wyjątek - jeden z siedmiu. Innymi słowy, uprawnionym jest przypuszczenie, że liczba podmiotów podlegających NIS II ulegnie istotnemu przyrostowi. Z jednej strony to dobrze, bo oprogramowanie złośliwe nie rozróżnia wielkości przedsiębiorstwa podczas ataku. Z drugiej jednak strony wychodzi na to, że wiele przedsiębiorstw nie objętych obecnie obowiązkami KSC, będzie musiało poważnie przemyśleć swoje podejście do zagadnienia cyberbezpieczeństwa. Dwa omówione wyżej obszary, nie stanowią pełnej listy proponowanych zmian. W NIS II znalazł się jeszcze zapis o możliwości nakładania przez państwa członkowskie wymogów stosowania określonych norm europejskich, co było postulowane od dawna przez wielu specjalistów. Znalazły się zapisy odnośnie koordynacji działań w zakresie oceny ryzyka związanego z określonymi łańcuchami dostaw, czego przedsmak mieliśmy już przy okazji analizy ryzyka związanego z dostawami elementów dla sieci 5G. Mamy też, co o dziwo może okazać się bardzo dobrym i praktycznym rozwiązaniem, obowiązek przechodzenia szkoleń z zakresu cyberbezpieczeństwa przez osoby zarządzające przedsiębiorcami. Oczywiście od projektu do implementacji do porządku krajowego dzielą nas jeszcze mniej więcej dwa lata. Ale należy pamiętać, że poprzednia dyrektywa była dość pojemna i wiele elementów z propozycji NIS II może być wdrożone już teraz, bez czekania na uchwalenie dyrektywy i wejście jej w życie. Z drugiej strony, może pojawić się pytanie: czy za dwa lata, tak zmieniona dyrektywa będzie w dalszym ciągu adekwatna do poziomu ówczesnego poziomu rozwoju cyfrowej gospodarki? Kilka kwestii wydaje się jednak pewne. Zmiany nadchodzą. Kary ulegną zwiększeniu i będą nakładane tak jak ma to miejsce w przypadku RODO. Regulator dostanie daleko idące uprawnienia. A cyberprzestępcy nie zrezygnują z bajecznego interesu. Warto więc zacząć patrzeć na nakłady na cyberbezpieczeństwo nie jako na koszt (co obecnie dominuje), tylko jako na inwestycję w ochronę przychodów.

Irek Piecuch
Senior Partner DGTL Kibil Piecuch I Wspólnicy

AUTORZY RAPORTU:

Irek Piecuch
Senior Partner DGTL Kibil Piecuch I Wspólnicy
ireneusz.piecuch@dgtl.law

Bartosz Ulczycki
Associate DGTL Kibil Piecuch I Wspólnicy
bartosz.ulczycki@dgtl.law

Łukasz Masztalerz
Associate DGTL Kibil Piecuch I Wspólnicy
lukasz.masztalerz@dgtl.law

August Żywczyk
Member of the Board
a.zywczyk@defence24.pl

Nikola Bochyńska
Redaktor Naczelna CyberDefence24.pl
n.bochynska@defence24.pl

O DGTL

Kancelaria DGTL Kibil Piecuch i Wspólnicy S.K.A. to autorski projekt Irka Piecucha i Michała Kibila. Zbudowany przez nich zespół prawników, doradców i konsultantów to specjaliści zafascynowani możliwością twórczego stosowania prawa w rozwoju przedsiębiorstw wchodzących na ścieżkę transformacji cyfrowej. Tłumaczenie projektów budowy nowoczesnych relacji międzyludzkich w przedsiębiorstwach to zadanie, które DGTL wykonuje każdego dnia. Podobnie jak tłumaczenie na język prawny strategii firm pragnących zmienić świat, ale także tych, które z trudem uczą się cyfrowego języka.

Tradycyjne podziały obszarów wsparcia prawnego przechodzą już do lamusa. Opis obszarów, w których się specjalizujemy ujmujemy zatem nieco inaczej niż większość kancelarii starając się oddać ducha postępującej konwergencji różnych dziedzin prawa. Nasza działalność skupia się wokół trzech podstawowych wymiarów podzielonych na obszary branże oraz praktyki.

Obszary naszej specjalizacji to cyfryzacja, inwestycje, ludzie oraz kreacja. Branże, które wspieramy to IT, medialna, telekomunikacyjna oraz sportowa. Nasze wiodące praktyki odnoszą się do compliance, podatków i sporów.

Jako zespół łączy nas wspólny zestaw wartości, którymi postanowiliśmy kierować się w naszej kancelarii. Jesteśmy zdeterminowani, aby jedną z nich był wzajemny szacunek i tolerancja dla naszych indywidualnych przekonań. Pracujemy dla Fundacji Teatr 21, Fundacji Koźmińskich i fundacji a/typowi. Nie tak dawno adoptowaliśmy jeden z obrazów Muzeum Narodowego w Warszawie, autorstwa Maksymiliana Gierymskiego, a także sprawujemy mecenat nad jednym z najciekawszych artystów młodego pokolenia. Nasi prawnicy zasiadają w Radzie Powierniczej Akademii im. Leona Koźmińskiego, Międzynarodowej Radzie Konsultacyjnej Kolegium Prawa ALK, Radzie Programowej Fundacji „Czytamy" i radach programowych wielu konferencji prawniczych i branżowych odbywających się co roku w Polsce.

Raport „Zwarci, silni, gotowi? Polskie firmy w obliczu cyberzagrożeń." jest naszym 3 raportem. Więcej naszych publikacji odnajdziecie Państwo na naszej stronie www.dgtl.law. Zapraszamy także do śledzenia naszego profilu na LinkedIn https://www.linkedin.com/company/dgtllaw/ na którym codziennie pojawiają się ciekawe artykuły i informacje z zakresu naszych specjalizacji!

www.dgtl.law

O CyberDefence24.pl

CyberDefence24.pl to wiodący polski portal poruszający problematykę cyberbezpieczeństwa, cyfryzacji i technologii, którego celem jest informowanie i edukowanie odbiorców w dziedzinie cybersecurity.

Dziennikarze portalu codziennie dostarczają unikalne treści: najważniejsze wiadomości z branży, raporty i komentarze oraz rozmawiają z ekspertami, by przybliżać tematy związane z ochroną danych, prywatnością i innowacjami, zważając na kluczowe aspekty w kontekście gospodarczym i politycznym.

Serwis CyberDefence24.pl stawia na wielokanałową komunikację, w tym autorskie materiały wideo, wywiady z ekspertami i m.in. relacje z najważniejszych konferencji branżowych. Śledzenie na bieżąco wydarzeń sprawia, że publikowane artykuły prezentują zagadnienia w sposób problemowy i wielowymiarowy.

Technologia, bezpieczeństwo informacyjne, innowacyjne rozwiązania w armii i służbach, dezinformacja oraz fake newsy, prywatność i ochrona danych, nowoczesne produkty w cyberbezpieczeństwie – to nieobce redakcji tematy. W tygodniu najświeższe wiadomości, w weekendy – pogłębione analizy w ramach #CyberMagazynu. Zmiany w serwisie wprowadzane są pod hasłem #CyberIsFuture.

www.cyberdefence24.pl

CyberDefence 24

Defence24 Sp. z o.o.
ul. Foksal 18
00-372 Warszawa
Tel.: +48 22 890 02 95
www.cyberdefence24.pl

DGTL

DGTL Kibil Piecuch i Wspólnicy S.K.A.
ul. Kazimierzowska 43 lok. 49
02-572 Warszawa
Tel. +48 22 848 71 22
www.dgtl.law