ZARZĄDZANIE BEZPIECZEŃSTWEM DANYCH W PRZEDSIĘBIORSTWACH MSP Z UWZGLĘDNIENIEM CZYNNIKA LUDZKIEGO — WYNIKI BADAŃ

https://doi.org/10.33141/po.2018.08.07

Przegląd Organizacji, Nr 8 (943), 2018, ss. 44-52
www.przegladorganizacji.pl

Paweł Kobis, Artur Kisiołek

Wprowadzenie

Liczba danych na świecie wzrasta bardzo dynamicznie. Z przeprowadzonego w 2017 roku badania przez firmę IDC na zlecenie jednego z największych producentów pamięci masowych – firmy Seagate (Reinsel i in., 2017, s. 3) – wynika, że do 2025 roku światowe bazy danych osiągną wielkość 163 zettabajtów – jest to dziesięciokrotny wzrost w stosunku do dzisiejszych wartości. W 2016 roku liczba ta wynosiła bowiem 16,1 ZB. Badania te z jednej strony pozwalają przedstawić nowe możliwości, kreując wizję liderów biznesu, którzy będą mogli korzystać z nowych i wyjątkowych możliwości biznesowych opartych na bogactwie danych i wglądu, jaki zapewnia. Z drugiej strony prognozują problemy, jakie pojawią się z wyborem gromadzenia, lokalizacji i zabezpieczania takiej ilości danych. Przewiduje się również, że głównymi twórcami danych w podmiotach gospodarczych będą początkowo konsumenci, a do 2025 roku to przedsiębiorstwa będą odpowiedzialne za stworzenie 60% światowych zasobów cyfrowych.

Większość przetwarzanych przez podmioty gospodarcze danych wymaga ochrony. Przy tak dużym wzroście ich ilości niezbędne staną się systemy autonomiczne wspierające kontrolowane przez człowieka zabezpieczenia. Konieczny będzie również wzrost szkoleń dla kadry pracowniczej, eliminujący braki wiedzy w zakresie wciąż nowo powstających technik, technologii i zagrożeń cyfrowych. Biorąc pod uwagę współcześnie istniejące braki w procesach bezpieczeństwa danych wśród przedsiębiorstw, to zakładając trafność prognoz na najbliższe lata, należy spodziewać się dużych wyzwań stojących przed menedżerami działów IT organizacji gospodarczych.

W artykule nakreślono kwestię bezpieczeństwa zasobów informacyjnych jako jednego z głównych źródeł utrzymania przewagi konkurencyjnej na rynku gospodarczym i potencjału podmiotu gospodarczego w turbulentnym otoczeniu. Celem opracowania jest przedstawienie wyników badań będących fragmentem przeprowadzonych przez autorów badań ankietowych na przełomie 2016 i 2017 roku na temat aspektów bezpieczeństwa przetwarzania danych w przedsiębiorstwach z sektora MSP. Głównym problemem naukowym było z kolei wypracowanie ogólnego algorytmu postępowania w procesach związanych z zapewnieniem bezpieczeństwa informacyjnego z uwzględnieniem wszystkich zasobów cyfrowych podmiotów gospodarczych oraz tzw. „danych wrażliwych".

Rodzaje danych przetwarzanych w przedsiębiorstwach

Aby ogólnie sklasyfikować dane przetwarzane w przedsiębiorstwach wymagające określonego poziomu wiedzy, można podzielić je na następujące kategorie:

- związane z procesami: produkcyjnym, handlowym, usługowym;
- dane osobowe zwykłe;
- związane z procesem finansowo-księgowym;
- związane z procesem kadrowo-płacowym;
- dane osobowe wrażliwe, wynikające ze specyfiki prowadzenia działalności.

Pierwszy rodzaj danych występuje praktycznie w każdym podmiocie gospodarczym. Są to dane opisujące wytwarzane produkty, procesy produkcyjne (w postaci tekstu, grafiki, animacji), patenty, przepisy, receptury, procedury itp. Wraz z szeroko pojętym kapitałem intelektualnym stanowią kluczowy zasób organizacji, fundament prowadzenia działalności gospodarczej, który w wielu przypadkach trudny jest do oszacowania i wyceny (Kłosowski i in., 2017, s. 45, 46). W systemie sieciowej komunikacji multimedialnej są podstawowym warunkiem sukcesu (Kiełtyka, 2017, s. 34). Bardzo często objęte są tajemnicą i określonym poziomem dostępności dla poszczególnych pracowników przedsiębiorstwa. Jakakolwiek utrata tych danych wiąże się z obniżeniem konkurencyjności, a w przypadkach skrajnych upadkiem podmiotu gospodarczego. Część tych danych, informacji może być również przechowywana w postaci tradycyjnej, papierowej lub tzw. wiedzy ukrytej, istniejącej tylko jako intelektualny potencjał wybranych pracowników lub właściciela przedsiębiorstwa.

Dane osobowe oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Definicja ujęta w rozporządzeniu RODO jest dość ogólna, a kryterium, według którego można zaliczyć informację do określonej kategorii danych, nie jest uniwersalne. Dane osobowe mogą przybierać różne formy: tekstu, filmu, zdjęcia, danych biometrycznych (Sumińska, Postuła, 2017, s. 108). Artykuł 4 rozporządzenia RODO określa możliwą do zidentyfikowania osobę fizyczną jako taką, którą „można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny,

dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej". Dane osobowe zwykłe w przedsiębiorstwie dotyczą: kontrahentów, klientów, pracowników oraz wszystkich podmiotów gospodarczych współpracujących z przedsiębiorstwem na poszczególnych szczeblach zarządczych, działach produkcyjnych, handlowych i usługowych.

Dane związane z procesem finansowo-księgowym stanowią zasoby wynikające z ustawy o rachunkowości z dnia 29 września 1994 r. (Ustawa …, 1994). W myśl zacytowanej ustawy przedsiębiorstwa muszą przechowywać te dane minimum 5 lat. Jest to więc zasób, który powinien mieć zaimplementowane określone rozwiązania z zakresu archiwizacji. Podobnie, dane kadrowo-płacowe muszą być przechowywane przez okres 50 lat, co wynika z art. 51u ust. 1 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz.U. z 2018 r., poz. 217 t.j.) (Ustawa …, 1983). Dane te przechowywane są najczęściej w podmiotach gospodarczych w postaci baz danych stanowiących źródło dla systemów informatycznych zarządzania, np. klasy ERP. Zapewniają one lepszą integrację rachunkowości finansowej, zorientowanej na transakcje gospodarcze i rachunkowości zarządczej ukierunkowanej na analizę ekonomiczną (Dyczkowski, Dyczkowska, 2014, s. 110).

Wymagającym szczególnej ochrony są dane tzw. „wrażliwe" lub według nowej nomenklatury RODO dane „szczególnie chronione". Nie są to zwykle dane o charakterze strategicznym dla przedsiębiorstwa, lecz zgodnie z obowiązującym prawodawstwem wymagają stosowania najbardziej zaawansowanych zabezpieczeń. Dane szczególnie chronione, w myśl rozporządzenia z dnia 27 kwietnia 2016 roku a obowiązującego od 25 maja 2018 roku (Rozporządzenie Parlamentu …, 2016), to:

- Dane o stanie zdrowia;
- Dane ujawniające pochodzenie rasowe lub etniczne;
- Poglądy polityczne;
- Przekonania religijne;
- Światopogląd;
- Przynależność do związków zawodowych;
- Dane genetyczne;
- Dane biometryczne (co obejmuje np. głos, odciski palców, obraz twarzy);
- Dane dotyczące seksualności;
- Dane dotyczące orientacji seksualnej.

Praktycznie wszystkie przedsiębiorstwa gospodarcze przetwarzają dane sensytywne w minimalnym stopniu. Dotyczy to przykładowo działu kadr, który dysponuje danymi ze zwolnień lekarskich, na których widnieje kod chorobowy, informacji o ciąży pracownicy (np. art. 185 Kodeksu pracy) (Mazur-Zych, 2016), przynależność do związków zawodowych oraz wybrane dane biometryczne, służące, szczególnie w większych podmiotach gospodarczych do identyfikacji pracownika na stanowisku komputerowym lub przy identyfikacji dostępu do określonych pomieszczeń (np. odcisk palca, obraz twarzy).

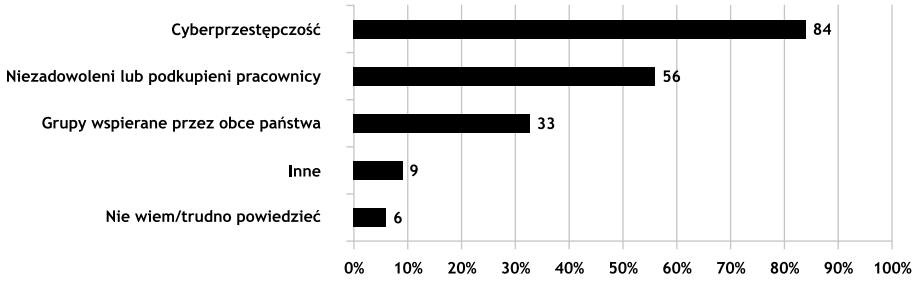
Wszystkie wymienione kategorie danych wymagają szczególnego traktowania w aspekcie ich bezpieczeństwa. W podmiotach gospodarczych należy podejmować próby maksymalizacji zabezpieczeń ze szczególnym uwzględnieniem systemów informatycznych jako dominujących w zakresie narzędzi przetwarzania informacji.

Wybrane aspekty bezpieczeństwa danych w przedsiębiorstwach związane z czynnikiem ludzkim

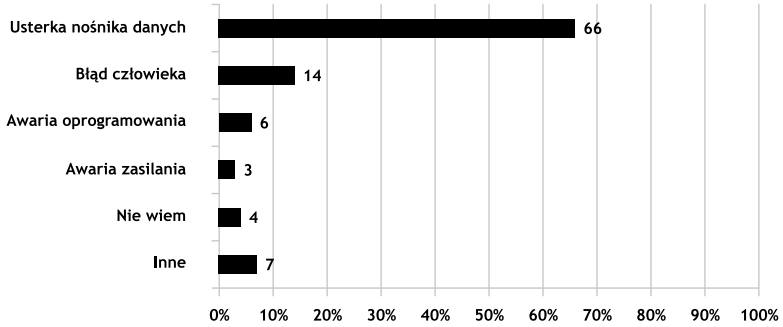
System zarządzania informacją w przedsiębiorstwie oprócz takich elementów, jak: tradycyjne formy przetwarzania informacji, systemy informatyczne, składa się również z tzw. czynnika ludzkiego. Człowiek, najczęściej pracownik danego przedsiębiorstwa, jest jednym z ważniejszych „elementów" odpowiedzialnych za bezpieczeństwo informacji (Kobis, Dudek, 2017, s. 12, 13) . Istnieje szereg badań i opracowań naukowych skłaniających się ku tezie, że to człowiek jest jednym z najsłabszych i jednocześnie najistotniejszych ogniw bezpieczeństwa informacji w podmiocie gospodarczym (Pańkowska, 2004; Żurakowski, 2015; Staniewska, 2015). W jednym z ostatnich badań przeprowadzonych przez jedną z największych firm produkujących oprogramowanie zabezpieczające: Kaspersky Lab. we współpracy z firmą badawczą B2B International, na próbie 5000 firm na całym świecie, ujawniono, że (Kaspersky Team, 2017):

- 46% incydentów zarejestrowanych w 2016 roku było związanych z przypadkowym naruszeniem zasad cyberbezpieczeństwa w firmie przez pracowników;
- 53% infekcji związanych ze szkodliwym oprogramowaniem spowodowanych było działaniem nieuważnego pracownika;
- 36% ataków związanych ze szkodliwym oprogramowaniem związanych było z działaniem socjotechnicznym, czyli celowym zmanipulowaniem pracownika;
- W 40% przypadków pracownicy próbowali ukryć incydent, przez co zwiększali szkodę i narażali firmę na jeszcze większe problemy z bezpieczeństwem;
- Niemal 50% ankietowanych obawia się, że ich pracownicy poprzez nieumyślne użycie urządzeń mobilnych mogą ujawnić informacje firmy.

W styczniu 2018 roku jedna z największych firm audytorsko-doradczych na świecie – KPMG – opublikowała raport pt. „Barometr cyberbezpieczeństwa. Cyberatak zjawiskiem powszechnym", w którym zdiagnozowano bieżące trendy i podejście polskich przedsiębiorstw w zakresie ochrony informacji na płaszczyźnie elektronicznego przetwarzania danych. Badaniu poddano ponad 100 małych, średnich i dużych przedsiębiorstw. Pytania skierowane były do osób zajmujących kluczowe stanowiska w działach odpowiedzialnych za bezpieczeństwo informacji (Kurek, Radziwon, 2018). W jednym z pytań dotyczących realnych zagrożeń dla firm respondenci udzielili odpowiedzi, że aż 56% potencjalnych zagrożeń może pochodzić od niezadowolonych lub podkupionych pracowników (rys. 1).



Rys. 1. Które z poniższych grup lub osób stanowią realne zagrożenie dla firm?
źródło: opracowanie własne na podstawie (Kurek, Radziwon, 2018)



Rys. 2. Przyczyny utraty danych
Źródło: (Margol i in., 2017, s. 32)

Zagrożenia związane z czynnikiem ludzkim w organizacjach sektora MSP można rozważać ponadto w takich kategoriach, jak:

- Możliwość kradzieży danych przez pracowników lub osoby trzecie poprzez zewnętrzne pamięci przenośne;
- Niedostateczne zabezpieczenia na urządzeniach mobilnych podłączanych do sieci firmowych LAN;
- Otwieranie podejrzanych wiadomości e-mail i ich załączników;
- Instalowanie aplikacji niewiadomego pochodzenia.

Zagrożenia w aspekcie czynnika ludzkiego to również brak świadomości związanej z koniecznością tworzenia kopii zapasowych danych, ryzyko przypadkowego usunięcia danych z roboczych zasobów dyskowych oraz ryzyko nieświadomego udostępnienia danych.

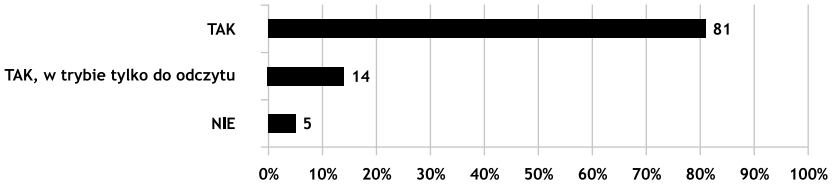
Kopie zapasowe stanowią w przeważającej liczbie przypadków jedyne źródło przywrócenia danych. Dlatego losowa awaria systemów przechowywania danych bez mechanizmu backupu i archiwizacji może doprowadzić do paraliżu pracy przedsiębiorstwa, przestojów w pracy, narazić podmiot gospodarczy na wysokie koszty finansowe. Konsekwencją pośrednią może również być utrata zaufania przez klientów i zaufania wewnętrznego w firmie (Margol i in., 2017, s. 32). Należy rozpatrywać więc zagadnienia związane z:

- tworzeniem kopii zapasowych z urządzeń roboczych i serwerów;
- tworzeniem kopii na nośnikach niebędących na stałe podłączonych do sieci LAN przedsiębiorstwa;
- likwidacją (profesjonalne usuwanie) danych i ich fragmentów zapisu bitowego z nośników podlegających utylizacji.

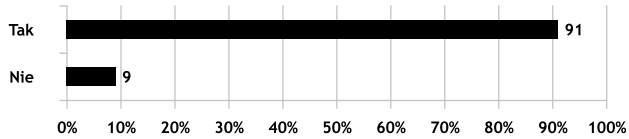
Ryzyko utraty danych w podmiocie gospodarczym wiąże się również z błędami wynikającymi z nieumiejętnej obsługi systemów bazodanowych. Brak dostatecznej ilości szkoleń, niski poziom kwalifikacji kadry lub błędy w procesach przyznawania uprawnień mogą przyczynić się do awarii baz danych organizacji gospodarczej. Na rysunku 2 przedstawiono najczęściej występujące przyczyny awarii informatycznych systemów magazynujących informacje w postaci elektronicznej. Błąd człowieka to druga w kolejności przyczyna utraty danych w organizacjach gospodarczych.

Wyniki badań

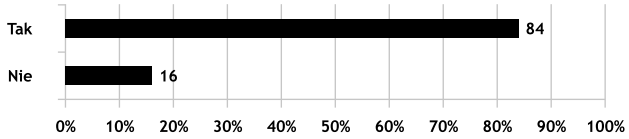
Badania zostały przeprowadzone w okresie od października 2016 roku do marca 2017 roku na próbie 153 przedsiębiorstw w województwie śląskim za pomocą ankiety elektronicznej przy użyciu metody CAWI (ang. Computer-Assisted Web Interview). Przedsiębiorstwa należały do sektora MSP, w tym mikro – 83 podmioty gospodarcze, małe – 59 podmiotów gospodarczych i 13 podmiotów średniej wielkości. Podział na wielkość przedsiębiorstw został oparty o obowiązujące obecnie Rozporządzenie Komisji Europejskiej określające m.in. definicję MSP nr 651/2014 z dnia 17 czerwca 2014 r. (Dziennik Urzędowy Unii Europejskiej, 2014) (Rozporządzenie Komisji, 2014). Przedstawione wyniki stanowią fragment obszerniejszych badań, które dotyczyły szerokich aspektów bezpieczeństwa informacji w organizacjach gospodarczych. Pytania skierowane były bezpośrednio do osób zajmujących się ochroną przetwarzania informacji w systemach informatycznych podmiotów gospodarczych.



Rys. 3. Czy system informatyczny funkcjonujący w sieci lokalnej pozwala na transmisję danych na urządzenia pamięci przenośnych?
Źródło: opracowanie własne



Rys. 4. Czy pracownicy korzystają z urządzeń mobilnych podłączonych do sieci lokalnej?
Źródło: opracowanie własne



Rys. 5. Czy urządzenia mobilne autoryzowane w sieci lokalnej są również używane poza nią?
Źródło: opracowanie własne

Zadane respondentom pytania dotyczyły zagadnień odnoszących się do zabezpieczeń eliminujących błędy związane z tzw. czynnikiem ludzkim w aspekcie ochrony danych.

W celu stworzenia bezpiecznego środowiska informatycznego, odpornego na tzw. „wyciek danych", należy ustalić hierarchię dostępu do zasobów informacyjnych oraz zabezpieczyć urządzenia komputerowe przed podłączaniem nieautoryzowanych pamięci przenośnych. W wyniku przeprowadzonego badania określono, że aż 81% przedsiębiorców posiada system, który bez przeszkód pozwala na przenoszenie danych na dowolny podłączony do stanowiska roboczego pendrive, kartę SD lub inny nośnik pamięci (rys. 3). Daje to nieograniczone możliwości kopiowania, kradzieży przez nieuczciwych, podkupionych pracowników danych i wynoszenia ich poza obręb sieci organizacji.

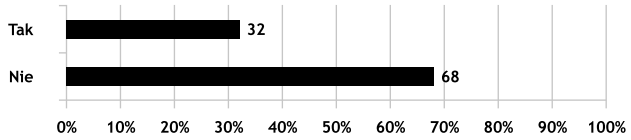
Stwarza się tym samym pole nadużyć do handlowania informacjami przedsiębiorstwa lub nieumyślnym rozpowszechnianiem ich w sieci globalnej (urządzenia przenośnej pamięci mogą służyć również do innych celów – np. prywatnych, można je również zagubić). Jedynie 5% przedsiębiorstw posiada politykę blokowania tego typu transmisji.

Podobny problem pojawia się podczas korzystania pracowników z urządzeń mobilnych. Urządzenia te stanowią coraz większą część ogólnie wykorzystywanych stanowisk roboczych. Obserwuje się ogromne tempo ich rozwoju w sensie ilości urządzeń, ilości i jakości dostępnych aplikacji, ich popularności, a także ich niewątpliwych cech pozytywnych – zapewniających szybki dostęp z niemal każdej lokalizacji (Chmielarz, Parys, 2017, s. 44). Aż 91% respondentów potwierdziło używanie ich w sieci LAN organizacji (rys. 4). Samo używanie laptopów, tabletów lub smartfonów nie stanowi zagrożenia samego w sobie, lecz używanie ich poza siecią może doprowadzić do sytuacji naruszających bezpieczeństwo danych. W 84% przypadków (rys. 5) urządzenia te są używane poza siecią organizacji, a więc istnieje ryzyko podłączenia ich do sieci bez zabezpieczeń, co może doprowadzić do zniszczenia informacji lub przejęcia ich przez osoby trzecie.

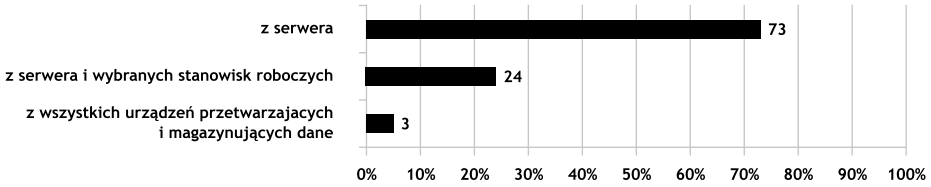
Jednym z najczęściej wymienianych zagrożeń związanych z czynnikiem ludzkim w aspekcie ochrony informacji jest nieumyślne uruchamianie załączników dołączanych do poczty elektronicznej pracowników oraz instalowanie przez nich oprogramowania niewiadomego pochodzenia lub oprogramowania typu freeware, adaware, które może zawierać kod szkodliwy dla komputera i sieci lokalnej. Nie istnieją obecnie zabezpieczenia programowe lub sprzętowe będące w stanie w 100% chronić zasoby informacyjne przed tego typu zdarzeniami. Rozwiązaniem może być blokowanie uprawnień do instalacji oprogramowania przez użytkowników komputerów oraz cykliczne szkolenia mające na celu podniesienie świadomości zagrożenia u osób przetwarzających dane elektroniczne (Kobis, 2017, s. 190, 191).

W badanych podmiotach gospodarczych aż 32% użytkowników ma uprawnienia do samodzielnego instalowania dowolnych aplikacji komputerowych (rys. 6).

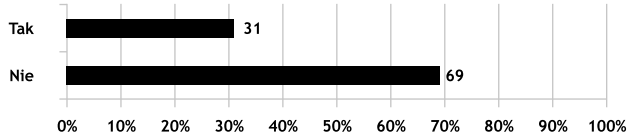
Poziom zaawansowania systemów zabezpieczeń w podmiotach gospodarczych jest dość silnie skorelowany z wielkością przedsiębiorstwa i jego możliwościami finansowymi. Stąd też przedsiębiorstwa mikro oraz małe mogą być bardziej narażone na utratę zasobów informacyjnych. Dlatego równolegle z udoskonalaniem



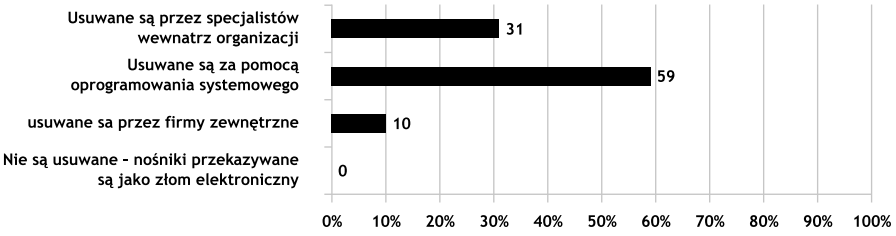
Rys. 6. Czy użytkownicy stanowisk roboczych mają uprawnienia do instalacji aplikacji i skryptów?
Źródło: opracowanie własne



Rys. 7. Z jakich urządzeń funkcjonujących w sieci lokalnej wykonuje się cykliczne kopie bezpieczeństwa?
Źródło: opracowanie własne



Rys. 8. Czy istnieje polityka tworzenia archiwów na nośnikach zewnętrznych, niepodłączonych na stałe do sieci LAN?
Źródło: opracowanie własne



Rys. 9. W jaki sposób niszczone są dane z nośników cyfrowych przeznaczonych do utylizacji?
Źródło: opracowanie własne

systemów bezpieczeństwa informacji należy tworzyć systematyczne kopie bezpieczeństwa przetwarzanych danych. Dane w przedsiębiorstwach, nawet tych posiadających serwery plików i bazy danych, są bardzo często magazynowane również na wszystkich stanowiskach roboczych, również tych mobilnych. Według przeprowadzonego badania, tylko 3% przedsiębiorców tworzy systematyczne kopie bezpieczeństwa z wszystkich urządzeń przetwarzających i magazynujących dane (rys. 7), a tylko 31% tworzy kopie bezpieczeństwa na nośnikach niepodłączonych na stałe do sieci lokalnej (rys. 8). Jest to wynik zły. Dane przechowywane w zasobach komputera roboczego lub urządzenia mobilnego są szczególnie narażone na ataki typu ransomware, czyli szyfrowania plików i żądania okupu za ich deszyfrowanie. Obecnie jedyną 100% ochroną przed tego typu atakami jest kopia bezpieczeństwa niepodłączona na stałe do sieci komputerowej. Oprogramowanie ransomware zaraża bowiem wszystkie dane na urządzeniach, które w sieci w danej chwili funkcjonują.

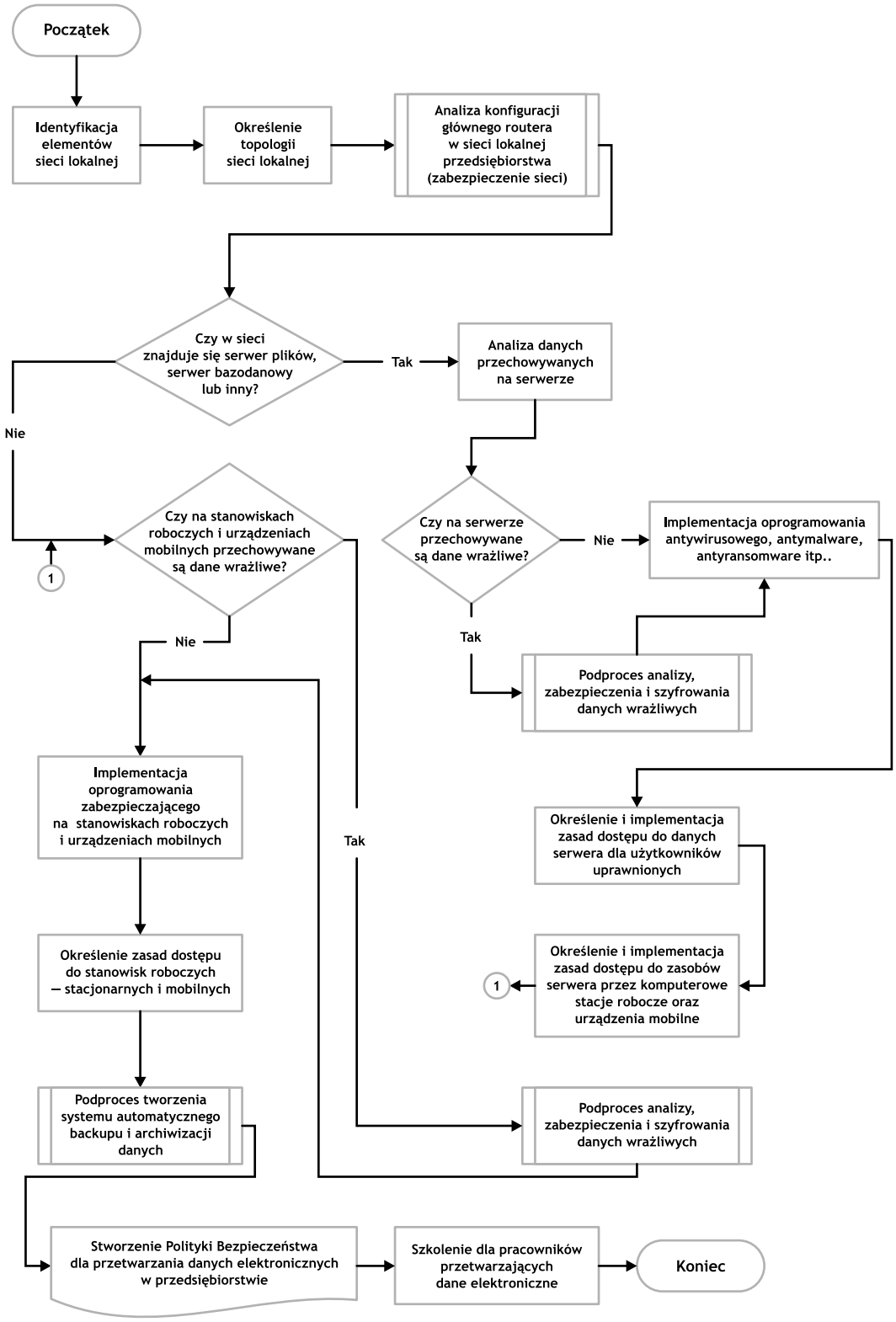
Tworzenie kopii bezpieczeństwa na nośnikach zewnętrznych jest najtańszym z punktu widzenia przedsiębiorstwa sposobem ochrony danych. Wymaga użycia zwykłych nośników optycznych (DVD, BR) lub dysków zewnętrznych HDD lub SSD. Brak tego typu zabezpieczenia świadczy więc o niskiej świadomości ryzyka wśród osób odpowiedzialnych za ochronę informacji, wpisując się w błędy tzw. czynnika ludzkiego.

Ochrona danych przedsiębiorstwa to również odpowiednia polityka związana z utylizacją zużytych nośników pamięci. Istniejące obecnie systemy i aplikacje informatyczne pozwalają na odzyskiwanie danych nawet po sformatowaniu dysków stałych lub zwykłym usunięciu plików za pomocą systemu operacyjnego.

Każdy nośnik pamięci przed właściwą utylizacją powinien zostać „wyczyszczony" z zachowaniem odpowiednich procedur minimalizujących ryzyko ponownego odczytania zawartości. Aż 59% badanych przedsiębiorstw nie stosuje określonych technik usuwania danych (rys. 9), przez co naraża się na możliwość przechwycenia informacji przez osoby lub podmioty nieupoważnione.

Ogólny schemat postępowania w celu zapewnienia bezpieczeństwa danych

Procesy związane z zabezpieczaniem danych w przedsiębiorstwach są mocno uzależnione od specyfiki danego podmiotu gospodarczego, jego funkcjonowania, sposobu zarządzania informacją oraz rodzaju przetwarzanych danych. Autorzy podjęli próbę stworzenia ogólnego schematu postępowania, który powinien stanowić podstawę podczas skomplikowanego szeregu działań zmierzających do ochrony zasobów informacyjnych organizacji gospodarczej (rys. 10).



Rys. 10. Ogólny schemat postępowania przy zabezpieczaniu informacji w sieci lokalnej
Źródło: opracowanie własne

Należy zaznaczyć, że schemat ten uwzględnia najczęściej występujące składniki sieci komputerowej w przedsiębiorstwach sektora MSP i dla bardziej rozbudowanej infrastruktury należy uwzględnić te elementy, których w schemacie brakuje.

Identyfikacja elementów jest pierwszym procesem, który należy przeprowadzić, aby określić słabe i mocne strony systemu przetwarzania informacji. Etap ten umożliwia wyselekcjonowanie tych części sieci, na które należy zwrócić szczególną uwagę podczas procesu zabezpieczania. Stanowi on również punkt wyjścia do opracowania topologii sieci lokalnej.

Jednym z najistotniejszych działań podejmowanych w aspekcie ochrony informacji jest odpowiednia konfiguracja urządzenia będącego łącznikiem sieci globalnej Internet i sieci lokalnej przedsiębiorstwa – routera. Konfiguracja tego urządzenia pozwala m.in. na sprecyzowanie usług, jakie będą uruchamiane w sieci, urządzeń, jakie będą do sieci przyłączane, konfigurację wirtualnych sieci prywatnych, usługi QoS (ang. Quality of Service) oraz ustawienie niezbędnych zabezpieczeń, np. firewall.

Kolejnym etapem jest określenie obecności serwerów w sieci przedsiębiorstwa. Poprzez precyzyjną analizę danych należy określić, czy w zasobach serwera pracownicy przedsiębiorstwa przechowują dane wrażliwe. Jeśli tak, dane te należy odpowiednio zabezpieczyć oraz dodatkowo zaszyfrować. Szyfrowanie danych zabezpiecza je przed próbą nieautoryzowanego dostępu oraz ewentualnej kradzieży dysku lub całego urządzenia. Istotną kwestią w konfiguracji zabezpieczeń serwera jest określenie odpowiednich praw dostępu dla użytkowników oraz urządzeń sieciowych. Proces ten eliminuje przypadkowe podłączenie urządzenia do zasobów serwera, a przez to minimalizuje ryzyko niepowołanego dostępu do danych lub ich utratę. Podobną procedurę należy przeprowadzić na wszystkich urządzeniach roboczych oraz urządzeniach mobilnych wykorzystywanych w przedsiębiorstwie.

Bardzo ważnym podprocesem w ogólnym schemacie postępowania przy zabezpieczaniu danych jest stworzenie odpowiednich mechanizmów automatycznego backupu (codziennego, cogodzinnego lub w czasie rzeczywistym) oraz systemu archiwizacji danych. Proces archiwizacji danych nie może być w pełni zautomatyzowany, gdyż z założenia powinien odbywać się na urządzeniu niepodłączonym do sieci lokalnej. W przedsiębiorstwach nieposiadających dużych zasobów danych archiwizacja może odbywać się na nośnikach optycznych (DVD, BR).

Programowo-sprzętowe zabezpieczenie obszaru przetwarzania informacji w podmiocie gospodarczym powinno zakończyć się opracowaniem odpowiedniej polityki bezpieczeństwa, z którą należy zapoznać każdego pracownika, który przetwarza dane. Prawidłowo przygotowana polityka bezpieczeństwa powinna zawierać takie elementy, jak:

- Wykaz budynków, pomieszczeń, w których przetwarzane są dane;
- Wykaz zbiorów danych oraz systemów informatycznych, które są używane do przetwarzania danych;
- Rodzaje użytych zabezpieczeń, zarówno fizycznych do ochrony budynku i pomieszczeń, jak i sprzętowych i programowych do ochrony samych danych;
- Opis środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Polityka bezpieczeństwa w aspekcie danych osobowych wraz z obowiązującym rozporządzeniem RODO nie jest dokumentem wymaganym. Stanowi jednak element „dobrej praktyki" i poświadcza, że przedsiębiorstwo należycie i w sposób odpowiedzialny traktuje zagadnienia związane z ochroną danych cyfrowych.

Ostatnim, lecz jednym z ważniejszych elementów schematu jest szkolenie pracowników. Biorąc pod uwagę tempo zmian w zakresie wykorzystywania nowych technologii oraz pojawiania się nowych zagrożeń informatycznych, szkolenia powinny odbywać się cyklicznie, przynajmniej raz w roku.

Przedstawiony schemat zakłada istnienie sieci lokalnej bez wykorzystywania serwerów zdalnych lub chmury obliczeniowej. W przypadku delegowania zasobów informacyjnych poza obszar sieci lokalnej należy zaimplementować odpowiednie mechanizmy kontroli tych zasobów oraz rozważyć tworzenie kopii lokalnych zasobów (Kobis, Chmielarz, 2017, s. 69).

Podsumowanie

Przetwarzanie danych we współczesnych organizacjach gospodarczych związane jest z użyciem nowych technologii i technik informatycznych. Dane w postaci zapisu bitowego przechowywane w plikach, bazach danych wymagają budowy specyficznego systemu ochrony, odmiennego od funkcjonującego w obszarze danych analogowych. Poruszone w artykule zagadnienia związane z bezpieczeństwem danych powinny stanowić punkt wyjścia w tworzeniu metod niwelujących ryzyka utraty zasobów informacyjnych, uważanych obecnie za jeden z głównych zasobów współczesnych przedsiębiorstw. Przeprowadzone przez autorów badania opisują jeden z obszarów związanych z bezpieczeństwem informacji, cechujący się dużym wpływem czynnika ludzkiego jako elementu odpowiedzialnego za prawidłowe przetwarzanie danych. Wśród badanych przedsiębiorstw można zauważyć znaczny niedomiar w aspekcie przestrzegania podstawowych zasad bezpieczeństwa. Może wynikać on z wielu czynników: braku odpowiednich środków finansowych przeznaczanych na doszkalanie kadry pracowniczej, braku świadomości, wiedzy w zakresie bezpieczeństwa wśród menedżerów, pracowników odpowiedzialnych za działy IT lub z bagatelizowania i lekceważenia zasad bezpieczeństwa w dynamicznie rozwijającym się świecie zagrożeń cyfrowych.

Prezentując ogólny schemat postępowania przy zabezpieczaniu informacji w sieci lokalnej, autorzy mieli na celu usystematyzowanie działań zmierzających do

zapewnienia bezpieczeństwa zasobów informacyjnych. Zaprezentowane w schemacie procesy stanowią elementarne minimum i powinny przyczynić się do wzmożenia działań w zakresie zapewnienia bezpieczeństwa sieciom lokalnym podmiotów gospodarczych. Należy również zaznaczyć, że schemat ten został stworzony w oparciu o analizę literaturową podmiotów z sektora MSP. Podmioty duże ze względu na złożoność występujących procesów wymiany informacji cechują się znacznie bardziej skomplikowanymi zasadami przetwarzania informacji.

dr inż. Paweł Kobis
Politechnika Czestochowska
Wydział Zarządzania
e-mail: pawel.kobis@wz.pcz.pl

dr inż. Artur Kisiołek
Wielkopolska Wyższa Szkoła Społeczno-Ekonomiczna w Środzie Wielkopolskiej
Wydział Ekonomiczny
e-mail: a.kisiolek@wwsse.pl

Bibliografia

[1] Chmielarz W., Parys T. (2017), *Uwarunkowania zastosowania handlu mobilnego*, „Przegląd Organizacji", Nr 8, s. 43–48.

[2] Dyczkowski T., Dyczkowska J. (2014), *Wpływ technologii informacyjnych na funkcjonowanie systemów sprawozdawczości zarządczej w polskich przedsiębiorstwach*, Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, Nr 344, s. 109–121.

[3] Dziennik Urzędowy Unii Europejskiej, L 187, Tom 57, 26 czerwca 2014, http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=OJ:L:2014:187:FULL&from=EN, data dostępu: 24.06.2018 r.

[4] Kaspersky Team, *Czynnik ludzki w bezpieczeństwie IT: jak pracownicy sprawiają, że firmy są podatne od wewnątrz* (2017), https://plblog.kaspersky.com/the-human-factor-in-it-security/7079/, data dostępu 17.06.2018 r.

[5] Kiełtyka L. (2017), *Narzędzia i technologie multimedialne wspomagające pracę menedżerów we współczesnych organizacjach*, „Przegląd Organizacji", Nr 8, s. 33–42.

[6] Kłosowski G., Paździor A. Rzemieniak M. (2017), *Zarządzanie aktywami niematerialnymi w systemach produkcyjnych*, „Przegląd Organizacji", Nr 7, s. 44–50.

[7] Kobis P. (2017), *Zarządzanie w zakresie bezpieczeństwa informacji w małych i średnich przedsiębiorstwach*, „Przegląd Nauk Ekonomicznych", Nr 27, s. 187–196.

[8] Kobis P., Chmielarz G. (2017), *The Barriers and Benefits of Implementing Cloud Computing in Economic Organizations*, „Informatyka Ekonomiczna", Nr 3(45), s. 66–79.

[9] Kobis P., Dudek D. (2017), *Poziom świadomości menedżerów w aspekcie ochrony danych elektronicznych w przedsiębiorstwach*, [w:] L. Kiełtyka, A. Sokołowski (red.), *Techniki i technologie wspomagające funkcjonowanie przedsiębiorstw*, Wydawnictwo Politechniki Częstochowskiej, Częstochowa, s. 11–20.

[10] Kurek M., Radziwon K. (2018), *Barometr cyberbezpieczeństwa. Cyberatak zjawiskiem powszechnym*, Raport KPMG, Międzynarodowa Grupa Sprawozdawczości Finansowej KPMG (ang. International Financial Reporting Group),. https://assets.kpmg.com/content/dam/kpmg/pl/pdf/2018/01/pl-Barometr-cyberbezpieczenstwa-cyberatak-zjawiskiem-powszechnym.PDF, data dostępu: 30.06.2018 r.

[11] Margol P., Dymora P. Mazurek M. (2017), *Strategie archiwizacji i odtwarzania baz danych*, Zeszyty Naukowe Politechniki Rzeszowskiej, z. 36(3), październik-grudzień, s. 31–41.

[12] Mazur-Zych A. (2016), *Co mówią przepisy o przetwarzaniu danych wrażliwych pracowników*, Portal poradyodo.pl, https://www.poradyodo.pl/dane-osobowe-a-prawo-pracy/co-mowia-przepisy-o-przetwarzaniu-danych-wrazliwych-pracownikow-7342.html, data dostępu: 29.06.2018 r.

[13] Pańkowska M. (2004), *Zabezpieczenie wiedzy w organizacjach gospodarczych*, Prace Naukowe Akademii Ekonomicznej we Wrocławiu, Nr 1011, s. 275–285.

[14] Reinsel D., Gantz J., Rydning J. (2017), *Data Age 2025: The Evolution of Data to Life-Critical Don't Focus on Big Data; Focus on the Data That's Big*, An IDC White Paper, Sponsored by Seagate, https://www.seagate.com/www-content/our-story/trends/files/Seagate-WP-DataAge-2025-March-2017.pdf, access date: 03.07.2018.

[15] Rozporządzenie Komisji (UE) Nr 651/2014 z dnia 17 czerwca 2014 r. uznające niektóre rodzaje pomocy za zgodne z rynkiem wewnętrznym w zastosowaniu art. 107 i 108 Traktatu, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32014R0651, data dostępu: 02.07.2018 r.

[16] 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), https://eur-lex.europa.eu/legal-content/pl/TXT/?uri=CELEX%3A32016R0679, data dostępu: 08.07.2018 r.

[17] Staniewska E. (2015), *Czynnik ludzki w zarządzaniu bezpieczeństwem informacyjnym badanych przedsiębiorstw*, Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, Nr 382, s. 389–400.

[18] Sumińska Z., Postuła I. (2017), *Wyzwania dla ochrony danych osobowych w obrocie gospodarczym przed wejściem w życie Rozporządzenia Ogólnego o Ochronie Danych Osobowych (RODO)*, Studia i Materiały, Wydział Zarządzania Uniwersytetu Warszawskiego, Nr 2, cz. 2, s. 106–118.

[19] Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach, Dz.U. 1983, Nr 38, poz. 173, http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19830380173, data dostępu: 07.07.2018 r.

[20] Ustawa z dnia 29 września 1994 r. o rachunkowości, Dz.U. 1994, Nr 121, poz. 591, http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19941210591, data dostępu: 07.07.2018 r.

[21] Żurakowski Z. (2015), *Kultura bezpieczeństwa w przedsiębiorstwie*, Zeszyty Naukowe Politechniki Śląskiej, seria: Organizacja i Zarządzanie, Nr 77, s. 323–330.

Data Security Management in SMEs with Human Factor Consideration

Summary

Widely understood information technologies presently constitute the main tool of information management in contemporary enterprises. Data, being a source of information is stored in designed for this purpose database systems, computer files placed on servers, desktop computers, mobile devices and external carriers. The aforementioned devices mostly operating in the local and global network are prone to cyberattacks aimed at stealing or removing data that has been recorded in them. The theoretical part of the paper presents selected issues in the scope of information security in enterprises of the SME sector. The authors' particular focus is so called human factor present in data protection processes. In the empirical part the primary goal of the paper is to present results of the research conducted in SME sector enterprises among IT infrastructure management staff and persons responsible for data protection. The second goal is to present the general procedure aimed at securing information in the local network of small and medium-sized enterprises.

Keywords

enterprise, information, data, security, human factor

* Tekst sponsorowany. *W artykule wykorzystano dane z raportu „Blockchain 2.0" przygotowanego przez Credit Suisse* https://research-doc.credit-suisse.com/docView?language=ENG&format=PDF&sourceid=csplusresearchcp&document_id=1080109971&serialid=pTkp8RFIoVyHegdqM8EllLNi1z%2Fk8mInqoBSQ5KDZG4%3D