Nowoczesne Systemy Zarządzania
Zeszyt 16 (2021), nr 4 (październik-grudzień)
ISSN 1896-9380, s. 55-66
DOI: 10.37055/nsz/147081

Instytut Organizacji i Zarządzania
Wydział Bezpieczeństwa, Logistyki i Zarządzania
Wojskowa Akademia Techniczna
w Warszawie

Modern Management Systems
Volume 16 (2021), No. 4 (October-December)
ISSN 1896-9380, pp. 55-66
DOI: 10.37055/nsz/147081

Institute of Organization and Management
Faculty of Security, Logistics and Management
Military University of Technology
in Warsaw

Bezpieczeństwo informacyjne procesów biznesowych w dobie pandemii COVID-19

Information security of business processes in the COVID-19 pandemic

Michał Jurek
Wojskowa Akademia Techniczna, Wydział Bezpieczeństwa, Logistyki i Zarządzania
michal.jurek@wat.edu.pl; ORCID: 0000-0003-0949-7458

Abstrakt. Pojawienie się koronawirusa i jego szybkie rozprzestrzenianie się po świecie zmusiło wiele podmiotów – prywatnych oraz publicznych – do zrewidowania filarów swojej działalności pod kątem możliwości ich przeniesienia do cyberprzestrzeni. Zmianę tę wymusiły coraz to nowsze regulacje wprowadzane przez decydentów celem walki z pandemią COVID-19. Ta transformacja objęła również procesy biznesowe, które są dzisiaj kluczowym czynnikiem umożliwiającym funkcjonowanie podmiotów biznesowych. Koniecznym zatem staje się zapewnienie im odpowiedniego poziomu bezpieczeństwa. Bez podjęcia działań prowadzących do zniwelowania poziomu ryzyka może dojść do ich zakłócenia, co skutkować będzie nie tylko obniżeniem sprawności funkcjonowania przedsiębiorstwa lub podmiotu z sektora publicznego, lecz nawet całkowitym wstrzymaniem jego działalności. Realizacja tego pesymistycznego scenariusza może negatywnie wpływać na ciągłość działania podmiotów zależnych, w tym również państwa. Należy zatem zbadać wpływ zagrożeń – również tych płynących z cyberprzestrzeni – na kształtowanie się poziomu bezpieczeństwa procesów biznesowych. Zagrożenia zaczęły bowiem występować coraz częściej, co ma związek z przejściem do trybu pracy zdalnej i digitalizacją większości działań podejmowanych przez pracowników. W XXI wieku, a w szczególności w dobie pandemii COVID-19, swobodny dostęp do zweryfikowanej i aktualnej informacji będzie stanowił podstawę do efektywnego planowania, projektowania oraz realizacji procesów biznesowych. Autor niniejszej pracy za pomocą kwerendy literatury oraz analizy danych zastanych (*desk research*) będzie starał znaleźć się odpowiedź na następujące pytanie: W jaki sposób na funkcjonowanie procesów biznesowych wpływa ich poziom bezpieczeństwa informacyjnego? Przeprowadzenie dokładnej analizy pozwoli na wskazanie działań zapobiegawczych, które należy wdrożyć, aby podnieść ogólny poziom bezpieczeństwa procesów biznesowych. Umożliwi to również utworzenie zbioru dobrych praktyk, który wspierać będzie decydentów (menedżerów) w przebiegu modelowania procesów biznesowych.
Słowa kluczowe: bezpieczeństwo informacyjne, procesy biznesowe, pandemia, COVID-19

Abstract. The appearance of the coronavirus and its rapid spread around the world forced many entities – private and public – to revise the keystone of their activities in terms of the possibility of their transfer to cyberspace. This change was forced by newer and newer regulations introduced by decision-makers in order to fight the COVID-19 pandemic. This transformation also included business processes, which are today a key factor enabling the functioning of business entities. Therefore, it becomes necessary to provide them with an appropriate level of security. Without taking actions to reduce the level of risk, they may be disrupted, which will not only reduce the efficiency of the operation of an enterprise or public sector entity, but also even stop its operations altogether. The implementation of this pessimistic scenario may have a negative impact on the continuity of operations of subsidiaries, including the state. Therefore, it is necessary to examine the impact of threats, including those from cyberspace, on the level of security of business processes. They (threats) began to occur more and more often, which is related to the transition to remote work and the digitization of most activities undertaken by employees. In the 21st century, and in particular in the time of the COVID-19 pandemic, free access to verified and up-to--date information will constitute the basis for effective planning, design and implementation of business processes. The author of this work with the help of a literature query and an analysis of existing data (desk research) will try to answer the following question – how does the level of information security affect the functioning of business processes? Carrying out a thorough analysis will allow to identify preventive actions that should be implemented to increase the overall level of security of business processes. It will also enable the creation of a set of good practices that will support decision-makers (managers) in the process of modeling business processes.
Keywords: information security, business processes, pandemic, COVID-19

Wstęp

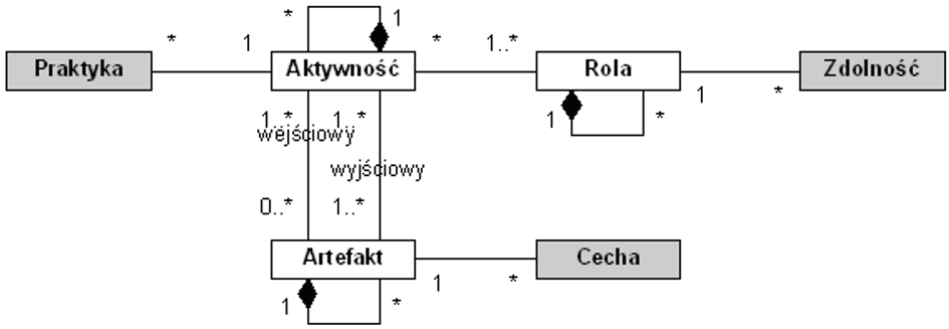
W erze gospodarki cyfrowej, silnie zorientowanej na pozyskiwanie i wykorzystywanie informacji – w szczególności przesyłanych za pomocą systemów informatycznych – podmioty prywatne oraz funkcjonujące w ramach sektora publicznego szczególną uwagę przywiązują do jej atrybutów jakości. Zapewnienie odpowiedniego poziomu cech informacji, takich jak poufność, dostępność oraz integralność (tzw. „Triada CIA"), będzie stanowić o „sile" jej jakości. Tylko informacje z wysokim wspomnianym współczynnikiem należy uwzględniać podczas planowania działalności organizacji. Podejmowanie działań na podstawie informacji o wątpliwej jakości może bowiem przyczyniać się do powstawania większej ilości zagrożeń, które to będą wpływać na ciągłość działania danego podmiotu oraz wszystkich elementów z nim powiązanych, które wchodzą w skład większej całości – systemu.

Informacja w istotny sposób będzie również wpływać na kształtowanie się i realizację procesów biznesowych. W silnie usieciowionym świecie i realiach gospodarki globalnej nawet najmniejszy podmiot gospodarczy może stać się kluczowym czynnikiem warunkującym kompletność łańcucha dostaw. Jego przerwanie może prowadzić do niedoboru odpowiednich środków, wykorzystywanych w ramach zaawansowanych procesów biznesowych (np. produkcyjnych). Przekładać się to będzie na możliwość powstania strat (w szczególności finansowych) znacznych rozmiarów.

Jak można zauważyć, działalność podmiotów z sektora prywatnego oraz publicznego opiera się w dużej mierze na wykorzystywaniu informacji do planowania celów oraz osiągnięcia już założonych. Muszą one więc poszukiwać ciągle nowych rozwiązań umożliwiających weryfikację jakości pozyskanej informacji. Zadanie to jednakże jest ogromnie trudne ze względu na bardzo szybko postępującą cyfryzację oraz digitalizację zarówno życia publicznego, jak i działalności służbowej. Do wymienionych czynników utrudniających ocenę jakości informacji należy zaliczyć również zjawisko danetyzacji (datafikacji). Próba całkowitej digitalizacji otaczającej nas rzeczywistości i jej kwantyfikacji będzie prowadzić do powstania szumu informacyjnego, który dodatkowo będzie utrudniał ocenę przydatności pozyskanej informacji (Śledziewska, 2020, s. 2). Będzie on powstawał ze względu na mnogość zagregowanych danych, których przetworzeniu pewne organizacje lub jednostki administracji publicznej nie będą mogły sprostać ze względów technicznych lub organizacyjnych. Pokaźna liczba jednostek zebranych danych utrudniać będzie również ich odpowiednie zabezpieczenie przed zagrożeniami płynącymi z cyberprzestrzeni, takimi jak chociażby *phishing*.

Procesy biznesowe

Na przestrzeni lat paradygmaty zarządzania organizacjami przeszły znaczące przemiany. Podejście tradycyjne, zakładające mocno zhierarchizowaną podległość służbową i pionowy rozkład pracy, zostało zastąpione podejściem procesowym (partycypacyjnym) (Peszko, 2002, s. 53). Charakteryzuje się ono poziomym rozkładem pracy, w którym wszystkie elementy (procesy) są ze sobą połączone i stanowią jedną całość (system) bez wyszczególniania relacji podwładny – przełożony.



Rys. 1. Uniwersalny model procesu
Źródło: Miler, Górski, 2020

Za podstawową cząstkę elementarną w podejściu procesowym przyjmuje się proces, który można charakteryzować przez pryzmat jego uniwersalnego modelu (rys. 1). Jak można zauważyć na powyższym rysunku, dzieli się on na dwie części: białą oraz szarą. Wszystkie elementy oznaczone kolorem białym muszą zaistnieć, aby można było mówić o uruchomieniu procesu. Można je zobrazować następująco jako (Zaskórski, 2012, s. 75):

- **aktywność** – są to podejmowane przez właściciela procesu wszystkie czynności, które prowadzą do wytworzenia artefaktu;
- **artefakt** – są to zasoby przetwarzane w ramach aktywności, stanowiące wynik działania (aktywności);
- **rolę** – stanowią ją zadania/instrukcje, które przyporządkowane są ogniwom uczestniczącym w danym procesie.

W celu oceny wymienionych komponentów zostały wyszczególnione elementy je charakteryzujące (szare) (Zaskórski, 2012, s. 76):

- **praktyka** – wszelkiego rodzaju kwalifikacje wymagane do zrealizowania aktywności;
- **cecha** – miary oceny w taksacji artefaktu;
- **zdolność** – ocena ogólnych predyspozycji do wykonywania określonej roli.

Na tej podstawie można więc stwierdzić, że procesy biznesowe to swoistego rodzaju algorytmy – ciągi działań lub procedur, które pozwalają osiągnąć założony cel z lepszym skutkiem (IBM, 2018). Mogą one podlegać ewaluacji pod kątem podnoszenia ich efektywności (Asseco, 2021). Ich efektywność bowiem będzie rzutować na produktywność całej organizacji. Modelując procesy biznesowe, należy zatem wziąć również pod uwagę dostęp do informacji, która w ich przypadku może przybierać formę nie tylko pewnych kompetencji osób odpowiedzialnych za ich wykonanie, lecz również wszelkiego rodzaju instrukcji, które warunkują skuteczne działanie systemów (np. informatycznych lub technicznych).

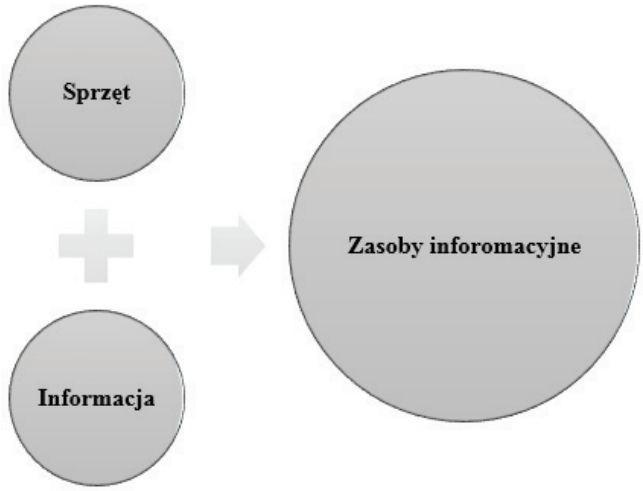
Bezpieczeństwo informacyjne

W XXI wieku dane oraz wynikające z nich informacje stały się swoistego rodzaju dobrem strategicznym. Dostęp do informacji i poprawne jej wykorzystanie może skutkować wykształceniem się przewagi konkurencyjnej. Koniecznym zatem staje się wdrożenie odpowiednich rozwiązań mających na celu jej zabezpieczenie.

Jednak, aby mówić o konkretnych metodach ochrony informacji, najpierw należy zdefiniować, czym jest bezpieczeństwo informacyjne. Samo bezpieczeństwo możemy definiować jako stan braku zagrożeń, które istotnie wpływałby na możliwość rozwoju jednostki lub podmiotu (w tym państwa). Zasoby informacyjne zaś są to wszelkiego rodzaju dobra materialne lub niematerialne (np. wiedza, licencje, sprzęt

komputerowy itd.), których zadaniem jest przesyłanie oraz przetwarzanie danych i informacji (Materska, 2005, s. 229-230). Zatem bezpieczeństwo informacyjne możemy definiować jako „brak zagrożeń dla informacji we wszystkich fazach ich wytwarzania, przetwarzania, przechowywania i przesyłania oraz zasobów informacyjnych mogących zakłócić swobodny rozwój społeczeństwa informacyjnego" (Aleksandrowicz, 2021, s. 84-84).

Wspomniany wyżej brak występowania ryzyk dla informacji i zasobów informacyjnych jest wynikiem działania zastosowanych zabezpieczeń do ich ochrony. Należy również zaznaczyć, że informacja wchodzi w skład zasobów informacyjnych (rys. 2).

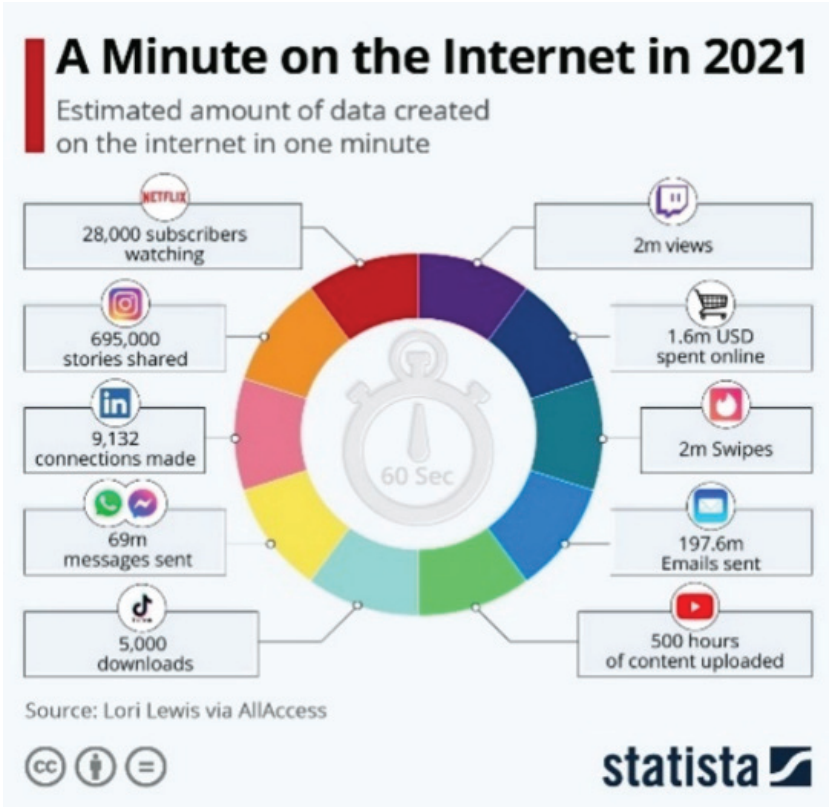


Rys. 2. Elementy składowe zasobów informacyjnych
Źródło: opracowanie własne

Jednakże trzeba ją rozpatrywać również jako całkowicie odrębne ogniwo. Wynika to z występowania tzw. metainformacji, czyli informacji o informacji. Ułatwia ona bowiem dostęp do właściwej informacji przez wstępną jej kategoryzację.

Bezpieczeństwo informacyjne a procesy biznesowe

W dobie pandemii COVID-19 digitalizacja procesów biznesowych przedsiębiorstw i jednostek administracji publicznej znacznie przyspieszyła. Wyraźnie pokazuje to rysunek 3.



Rys. 3. Dane wytworzone w ciągu 1 minuty w sieci Internet
Źródło: Jenik, 2021

Jak można zauważyć na powyższym rysunku, w ciągu jednej minuty w Internecie wygenerowano olbrzymi wolumen danych, w tym również transakcji, których łączna wartość wynosiła 1,6 mln dolarów amerykańskich. Obsługa tak wysokiej liczby danych w tak krótkim czasie wymaga zastosowania odpowiednich zabezpieczeń przed najczęściej wykorzystywanymi atakami cybernetycznymi oraz wydajnej infrastruktury sprzętowej.

Najczęstszymi typami cyberzagrożeń, z którymi muszą zmagać się przedsiębiorstwa, to (Wojciechowski, 2021, s. 105-106):

- **Malware** – złośliwe oprogramowanie w postaci skryptów lub aplikacji, a w szczególności tzw. Ransomware;
- **ataki socjotechniczne (*phishing*)** – wyłudzanie poufnych danych;
- **Man in the Middle** – podsłuchiwanie ruchu sieciowego (komunikacji) przez osobę trzecią;

- **DDoS (Distributed Denial of Service)** – zablokowanie możliwości korzystania z danego serwisu przez ciągłe wysyłanie dużej liczby zapytań do serwera;
- **SQL Injection** – odpytywanie (wstrzykiwanie poleceń) w sposób nieuprawniony bazy danych;
- **Cross-Site Scripting (XSS)** – umieszczenie kodu języka skryptowego w przeglądarce internetowej umożliwiającego zmianę treści lub sposobu jej działania;
- **Advanced Persistent Threat (APT)** – wielostopniowy atak hackerski, skrupulatnie przygotowywany umożliwiający dogłębną infiltrację wybranego celu.

Powyższe zestawienie uwidacznia to, że cyberprzestępcy dysponują dużym „arsenałem", który mogą wykorzystać do wykradania danych wrażliwych (np. danych badawczych) lub nawet prowadzenia działań z zakresu szpiegostwa gospodarczego. Kluczowym czynnikiem zatem staje się wprowadzanie odpowiednich rozwiązań techniczno-organizacyjnych celem zniwelowania prawdopodobieństwa wystąpienia wymienionych zagrożeń.

W pierwszej kolejności działania w tym kierunku powinny zostać podjęte przez decydentów z sektora rynków finansowych, handlu oraz szeroko pojętych mediów. Z tych gałęzi gospodarki w roku 2020 pochodziło najwięcej zgłoszeń dotyczących incydentów związanych z bezpieczeństwem informacji (kolejno 12,31%, 13,79% oraz 24,63%) (CERT Polska, 2021, s. 26). Ilustruje to rysunek 4.

W najmniejszym stopniu cyberzagrożeniami zostały dotknięte przedsiębiorstwa funkcjonujące w ramach następujących gałęzi gospodarki: gospodarka odpadami oraz rybołówstwo (po 0,01%), działalność ubezpieczeniowa (0,02%), izby gospodarcze i handlowe (0,03%), rolnictwo (0,04%), kultura i ochrona dziedzictwa narodowego (0,07%), wyznania religijne oraz mniejszości narodowe (0,08%) oraz wodociągi, turystyka i kultura fizyczna (po 0,09%) (CERT, 2021, s. 26). Rysunek 5 przedstawia podział incydentów ze względu na ich główne kategorie. Jak można zauważyć, największą grupę zarejestrowanych cyberzagrożeń stanowiły oszustwa komputerowe (79,75%), z tego aż 73,15% całości cyberataków stanowił *phishing*. Dużą grupę incydentów stanowiło użycie *malware* (złośliwego oprogramowania) – 7,16%. Najmniejszą grupę zarejestrowanych zagrożeń stanowią inne niesklasyfikowane cyberzagrożenia – 0,40%.

Sektor gospodarki	Liczba incydentów	%
Energetyka	101	0,97%
Transport	29	0,28%
Bankowość	1008	9,67%
Infrastruktura rynków finansowych	1283	12,31%
Służba zdrowia	112	1,07%
Wodociągi	9	0,09%
Infrastruktura cyfrowa	1016	9,75%
Inne	379	3,64%
Brak	0	0,00%
Administracja publiczna	388	3,72%
Budownictwo i gospodarka nieruchomościami	29	0,28%
Kultura i ochrona dziedzictwa narodowego	7	0,07%
Kultura fizyczna	9	0,09%
Oświata i wychowanie	71	0,68%
Rolnictwo	4	0,04%
Rybołówstwo	1	0,01%
Wyznania religijne i mniejszości narodowe	8	0,08%
Działalność ubezpieczeniowa	2	0,02%
Izby gospodarcze i handlowe	3	0,03%
Handel hurtowy i detaliczny	1437	13,79%
Produkcja	57	0,55%
Logistyka i dystrybucja	27	0,26%
Poczta i usługi kurierskie	500	4,80%
Turystyka	9	0,09%
Gospodarka odpadami	1	0,01%
Hotele	19	0,18%
Media	2568	24,64%
Usługi inne	384	3,69%
Osoby fizyczne	959	9,20%
Razem	10420	100,00%

Rys. 4. Incydenty obsłużone przez CERT Polska w 2020 r. w podziale na sektor gospodarki
Źródło: CERT Polska, 2021, s. 26

ıbraźliwe i nielegalne treści, w tym:	**371**	**3,56%**
ım	336	3,22%
ıkredytacja, obrażanie	8	0,08%
·nografia dziecięca, przemoc	1	0,01%
ısklasyfikowane	26	0,25%
Złośliwe oprogramowanie, w tym:	**746**	**7,16%**
ıus	0	0,00%
ɔak sieciowy	1	0,01%
ń trojański	10	0,10%
·ogramowanie szpiegowskie	1	0,01%
ler	0	0,00%
ɔtkit	0	0,00%
ısklasyfikowane	734	7,04%
Gromadzenie informacji, w tym:	**60**	**0,58%**
ınowanie	32	0,31%
dsłuch	0	0,00%
ynieria społeczna	1	0,01%
ısklasyfikowane	27	0,26%
Próby włamań, w tym:	**174**	**1,67%**
korzystanie znanych luk systemowych	5	0,05%
ıby nieuprawnionego logowania	14	0,13%
korzystanie nieznanych luk systemowych	0	0,00%
ısklasyfikowane	155	1,49%
Włamania, w tym:	**317**	**3,04%**
ımanie na konto uprzywilejowane	9	0,09%
ımanie na konto zwykłe	75	0,72%
ımanie do aplikacji	13	0,12%
	13	0,12%
sklasyfikowane	207	1,99%
Dostępność zasobów, w tym:	**121**	**1,16%**
k blokujący serwis (DoS)	0	0,00%
·proszony atak blokujący serwis (DDoS)	43	0,41%
ɔotaż komputerowy	0	0,00%
erwa w działaniu usług (niezłośliwe)	52	0,50%
sklasyfikowane	26	0,25%
Atak na bezpieczeństwo informacji, w tym:	**68**	**0,65%**
uprawniony dostęp do informacji	42	0,40%
uprawniona zmiana informacji	4	0,04%
ısklasyfikowane	22	0,21%
I. Oszustwa komputerowe, w tym:	**8310**	**79,75%**
ıuprawnione wykorzystanie zasobów	25	0,24%
·uszenie praw autorskich	2	0,02%
dzież tożsamości, podszycie się	11	0,11%
shing	7622	73,15%
ısklasyfikowane	650	6,24%
Podatne usługi, w tym:	**211**	**2,02%**
·arte serwisy podatne na nadużycia	29	0,28%
ısklasyfikowane	182	1,75%
nne	**42**	**0,40%**

Rys. 5. Incydenty obsłużone przez CERT Polska w 2020 r. w podziale na kategorie według taksonomii eCSIRT.net mkVI

Źródło: Incident Classification, 2015

Jak można zauważyć, podział występujących incydentów będzie znacząco zróżnicowany zależnie od sektora gospodarki oraz użytej metody ataku. Decydenci (menedżerowie) powinni zatem wdrożyć w pierwszej kolejności politykę bezpieczeństwa informacji (rozwiązanie organizacyjne), która będzie regulować metody postępowania z informacjami w trakcie nie tylko modelowania procesów biznesowych, lecz również w całym ich cyklu życia. Warunkować one będą także wprowadzane rozwiązania techniczne wymagane do odpowiedniego jej zabezpieczenia. Jednakże ciężar ochrony wrażliwych danych oraz informacji nie spoczywa wyłącznie na kadrze zarządczej, lecz również na każdym pracowniku. Powinni oni przestrzegać wszystkich zaleceń wydanych przez pracodawcę – właściciela procesów biznesowych. Człowiek jest bowiem najsłabszym ogniwem, które może zostać wykorzystane przez cyberprzestępców do pozyskania interesujących ich danych.

Wnioski

Procesy biznesowe stanowią w dzisiejszych czasach podstawowy filar działalności każdej organizacji. Kluczowym czynnikiem staje się więc konieczność zapewnienia im odpowiedniego poziomu ochrony również przed zagrożeniami płynącymi z cyberprzestrzeni. Będą one bowiem istotnie wpływać na ich efektywność oraz jakość. Obniżenie tych parametrów może w dłuższej perspektywie czasowej generować straty na różnych polach działalności danego podmiotu, co może skutkować zakłóceniem jego ciągłości działania (również informacyjnej), a w skrajnych przypadkach nawet jej przerwaniem. Chcąc nie dopuścić do materializacji cyberzagrożeń lub – jeśli już wystąpią – zniwelować ich skutki, koniecznym staje się wdrożenie odpowiednich regulacji organizacyjnych, np. w postaci różnego rodzaju zaleceń, oraz polityk i regulacji technicznych, np. w postaci wdrożenia do użytku w organizacji centralnie zarządzanego oprogramowania antywirusowego. Bezpieczeństwo informacyjne procesów biznesowych powinno leżeć w gestii każdego pracownika niezależnie od zajmowanego przez niego stanowiska. Od ich poziomu umiejętności cyfrowych bowiem będzie zależeć podatność procesów na cyberataki.

BIBLIOGRAFIA

[1] Aleksandrowicz, T., 2021. *Zagrożenia dla bezpieczeństwa informacyjnego państwa w ujęciu systemowym*, Warszawa: Difin.

[2] Materska, K., 2005. *Rozwój koncepcji informacji i wiedzy jako zasobu organizacji*, [w:] Sosińska-Kalata, B., Przastek-Samokowa, M. (red.), *Od informacji naukowej do technologii społeczeństwa informacyjnego*, Warszawa: Stowarzyszenie Bibliotekarzy Polskich.

[3] Peszko, A., 2002. *Podstawy zarządzania organizacjami*, Kraków: AGH.

[4] Wojciechowski, Z., 2021. *Wyzwania cyberbezpieczeństwa*, [w:] Gonciarski, W., Woźniak, J. (red.), *Bezpieczeństwo organizacji w warunkach gospodarki cyfrowej*, Warszawa: Difin.

[5] Zaskórski, P., 2012. *Asymetria w informacyjna w zarządzaniu procesami*, Warszawa: WAT.

NETOGRAFIA

[1] Asseco, 2021. https://pl.asseco.com/kariera/blog/jak-usprawnic-mojeklienta-procesy-biznesowe-4264/ (03.11.2021).

[2] CERT Polska, 2021. *Krajobraz bezpieczeństwa polskiego Internetu*, https://cert.pl/uploads/docs/Raport_CP_2020.pdf (03.11.2021).

[3] IBM, 2018. https://www.ibm.com/docs/pl/bpm/8.5.6?topic=designer-key-concepts-bpel-business-processes (03.11.2021).

[4] Incident Classification, 2015. https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf (03.11.2021).

[5] Jenik, C., 2021. *A Minute on the Internet in 2021*, https://www.statista.com/chart/25443/estimated-amount-of-data-created-on-the-internet-in-one-minute/ (03.11.2021).

[6] Miler, J., Górski, J., 2020. *Wzorce identyfikacji ryzyka w projektach informatycznych*, https://www.e-informatyka.pl/index.php/pimio/zapewnienie-jakosci/wzorce-identyfikacji-ryzyka-w-projektach-informatycznych/ (03.11.2021).

[7] Śledziewska, K., 2020. Dojrzałość cyfrowa w erze datafikacji i platformizacji, *Pomorski Przegląd Gospodarczy*. https://ppg.ibngr.pl/pomorski-przeglad-gospodarczy/dojrzalosc-cyfrowa-w-erze-datafikacji-i-platformizacji (03.11.2021).