Łukasz Dragun

Politechnika Białostocka
ORCID: 0000-0001-6768-6818

CYBERBEZPIECZEŃSTWO DANYCH SERWERA POCZTOWEGO KLUCZEM DO ROZWOJU PRZEDSIĘBIORSTW

Abstrakt

Cyberataki są zjawiskiem powszechnym wśród przedsiębiorstw działających w Polsce. 85% przedsiębiorstw odnotowało przynajmniej jeden cyberincydent w 2020 r. Zorganizowane grupy cyberprzestępcze i pojedynczy hakerzy są najczęstszymi źródłami ataków. Najgroźniejsze cyberzagrożenia dla przedsiębiorstw to: *malware* (APT, wycieki danych, *ransomware*), czynnik ludzki oraz ataki na aplikacje[1]. Zatrudnienie i utrzymanie wykwalifikowanych pracowników jest największym wyzwaniem w zakresie uzyskania oczekiwanego poziomu zabezpieczeń, istotniejszym nawet niż niewystarczający budżet. W Polsce blisko 40% przedsiębiorstw nie podejmuje działań związanych z RODO.

Celem niniejszej pracy jest próba identyfikacji potencjalnych cyberzagrożeń danych serwera pocztowego w przedsiębiorstwie z branży maszyn i urządzeń. Analizie zostały poddane rzeczywiste dane pracy serwera w jednym z podlaskich przedsiębiorstw. Zostały zaproponowane zalecenia ukierunkowujące na bezpieczeństwo danych serwerowych indywidualnych użytkowników.

• Słowa kluczowe: cyberbezpieczeństwo, ochrona danych, digitalizacja, zagrożenia bezpieczeństwa informacji.

[1] J.M.V. Cedeño, J. Papinniemi, L. Hannola, L. Donoghue, *Developing smart services by Internet of Things in manufacturing business*, „Lappeenranta University of Technology" 2018, Vol. 14(1), s. 59.

Abstract

Cyber-attacks are a common phenomenon among enterprises operating in Poland. 82% of enterprises experienced at least one cyber incident in 2017. Organized cybercriminal groups and single hackers are the most common sources of attacks. The most dangerous cyber threats for enterprises are malware (APT, data leaks, ransomware), the human factor and attacks on applications. Hiring and retaining skilled workers is the biggest challenge in achieving the expected level of security, even more than an insufficient budget.

The aim of this study is to try to identify potential cyber threats to mail server data in a company from the machinery and equipment industry. The actual data from server operations in one of Podlasie's enterprises were analysed. Recommendations aimed at the security of server data of individual users were proposed.

• Keywords: cybersecurity, data protection, digitization, information security threats.

Wstęp

Prowadzenie działalności gospodarczej opartej na teleinformatyzacji oprócz korzyści niesie również różnego rodzaju zagrożenia. Systemy informatyczne umożliwiają gromadzenie, przetwarzanie i szybkie udostępnianie danych w ramach przedsiębiorstwa, które mogą zostać użyte przeciw niemu, np. przez konkurencję[2]. Szpiegostwo przemysłowe jest ukierunkowane na zdobycie informacji i wykorzystanie ich w relacjach konkurencji np. cenowej na rynku[3]. Z uwagi na dynamiczny rozwój Internetu nadal jedną z podstawowych form do kontaktów biznesowych jest poczta elektroniczna. W nawiązaniu do celu pracy stwierdzić należy, iż korzystanie z poczty elektronicznej od zawsze

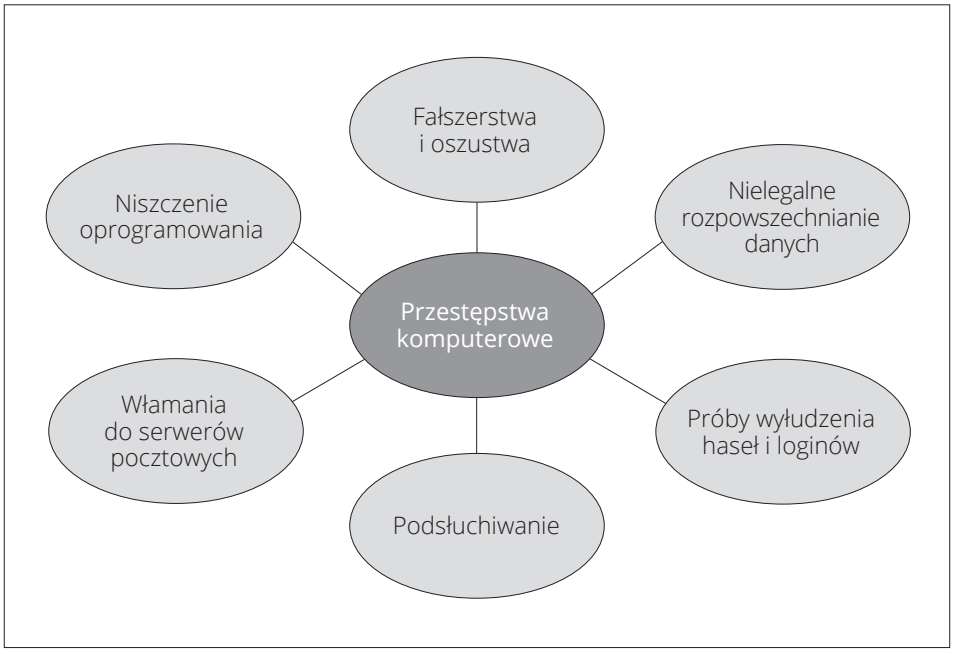
[2] K. Bielawski, M. Chmieliński, M. Pabich, *Zagrożenia bezpieczeństwa informacji oraz rozwiązania IT w zakresie wsparcia produkcji i logistyki w przedsiębiorstwie*, „Problems Mechatronics Armament, Aviation, Safety Engineering" 2017, t. 8, nr 4(30), s. 151.

[3] A. Patkowski, *„Cicha reakcja" na zdalne ataki teleinformatyczne*, „Przegląd Teleinformatyczny" 2017, t. 5, nr 3, s. 33.

budziło wiele wątpliwości co do bezpieczeństwa treści przechowywanych w skrzynkach pocztowych i ich prawidłowej konfiguracji na dedykowanych do tego różnych programach pocztowych.

Bezpieczeństwem informacyjnym jest również działanie, system bądź metoda, które zabezpieczają zasoby informacyjne gromadzone, przetwarzane, przekazywane oraz przechowywane w pamięci komputerów i sieciach teleinformatycznych[4]. Bezpieczeństwo jest procesem ciągłym, w ramach którego przedsiębiorstwa starają się udoskonalać mechanizmy zapewniające im poczucie bezpieczeństwa[5].

Rysunek 1. Schemat przestępstw komputerowych



Źródło: opracowanie własne na podstawie: K. Bielawski, M. Chmieliński, M. Pabich, op. cit., s. 153.

[4] H. Chen, *Theoretical foundations for cyber-physical systems: a literature review*, „Journal of Industrial Integration and Management" 2017, Vol. 2, No. 3, s. 1750013; H. Chen, *Applications of cyber-physical system: a literature review*, „Journal of Industrial Integration and Management" 2017, Vol. 2, No. 3, s. 1750012.

[5] K. Bielawski, M. Chmieliński, M. Pabich, op. cit., s. 154.

Miejscem, które wymaga szczególnego nakładu pracy w ramach bezpieczeństwa przesyłanych danych, są serwery pocztowe przeznaczone dla użytkowników danego przedsiębiorstwa.

Poczta elektroniczna jest powszechnie stosowanym narzędziem ułatwiającym komunikację i przekazywanie informacji w różnej formie cyfrowej[6]. Usługa ta stwarza wiele problemów w zakresie bezpieczeństwa, m.in.:

- serwer poczty może zostać zaatakowany przez hakera, a następnie posłużyć do włamania do sieci prywatnej,
- serwer poczty może zostać zablokowany za pomocą ataku *Denial of Service* (DoS) bądź ulec awarii,
- wiele groźnych aplikacji (np. wirusy, robaki, konie trojańskie) może przedostać się do sieci prywatnej poprzez wiadomości pocztowe,
- serwer poczty może odebrać wiele niepożądanych przesyłek pocztowych tzw. spamów,
- serwer poczty może zostać wykorzystany przez hakerów (nazywanych także lamerami) do wysyłania spamów do innych serwerów w Internecie,
- poufne informacje przesyłane za pomocą poczty mogą zostać odczytane przez osoby nieupoważnione bądź zmodyfikowane w niepożądany sposób,
- serwer DNS udostępniający informacje na temat serwera poczty może zostać zablokowany lub ulec awarii[7].

Co roku dochodzi do wielu cyberataków z powodu braku świadomości użytkowników Internetu oraz usług, jakie są świadczone w ramach dostępu do niego[8]. Ponadto internauci chętnie wymieniają się różnego rodzaju informacjami w przypadku bezpłatnej aplikacji, godne zaufania jest otwieranie

[6] L. Bosman, N. Hartman, J. Sutherland, *How manufacturing firm characteristics can influence decision making for investing in Industry 4.0 technologies*, „Journal of Manufacturing Technology Management" 2020, Vol. 31, No. 5, s. 117–114.

[7] M. Stawowski, *Praktyczne metody ochrony poczty elektronicznej*, http://www.iniejawna.pl/pomoce/poczta.html [dostęp: 1.04.2021].

[8] D. Bilefsky, *Hackers use new tactic at Austrian hotel: locking the doors*, „The New York Times", www.nytimes.com/2017/01/30/world/europe/hotel-austria-bitcoin-ransom.html?_r=0 [dostęp: 8.04.2021].

Wi-Fi i nadmierne udostępnianie informacji w mediach społecznościowych przy korzystaniu z tych samych haseł co do kont służbowych. Z powodu oszczędności użytkownicy prywatni unikają używania oprogramowania antywirusowego oraz chętniej klikają w linki z niezaufanych źródeł[9].

Celem niniejszej pracy jest próba identyfikacji potencjalnych cyberzagrożeń i ich konsekwencji w implementacji technologii Przemysłu 4.0 w przedsiębiorstwach produkcyjnych w obszarze wybranego przedsiębiorstwa z branży maszyn i urządzeń. Analizie zostały poddane rzeczywiste dane pracy serwera pocztowego z ukierunkowaniem na jego konfigurację, analizę funkcjonalną systemów centralnych oraz serwera pocztowego. W ostatniej części wskazane zostały zalecenia w celu zabezpieczenia i usprawnienia działania systemów centralnych oraz poczty elektronicznej przed cyberatakami.

Analiza funkcjonalna infrastruktury serwerowej

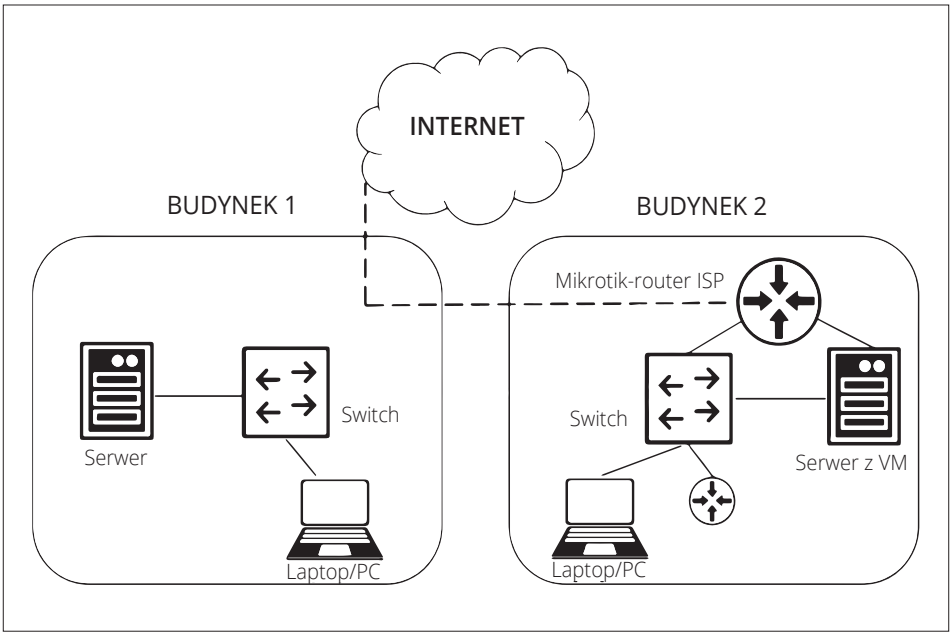
Infrastruktura informatyczna jednego z podlaskich przedsiębiorstw znajduje się w 9 lokalizacjach w Polsce i 3 za granicą. W głównej siedzibie przedsiębiorstwa znajdują się stacje robocze łączące się z routerem internetowym poprzez sieć przewodową i bezprzewodową. Na routerze zostały zainstalowane mechanizmy nadawania prywatnych adresów IP przeznaczonych dla urządzeń wewnątrz sieci (mechanizm DHCP). Komputery firmowe uzyskują adresy z podsieci.

Przedsiębiorstwo wykorzystuje systemy centralne (wspólne):

- serwer fizyczny z systemem serwerowym Windows Server 2019,
- serwer z VM – serwer fizyczny, którego głównym zarządcą jest VMware – za jego pomocą wydzielone są zasoby dla właściwych systemów – poszczególne serwery wirtualne nie widzą się inaczej niż przez sieć teleinformatyczną – zatem jeden z systemów nie ma dostępu bezpośrednio do danych innego.

[9] A. Tarabasz, *Cybersecurity and Internet of threats – new challenges in customer behavior,* „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2018, nr 360, s. 77.

Rysunek 2. Schemat infrastruktury serwerowej funkcjonującej w przedsiębiorstwie



Źródło: opracowanie własne.

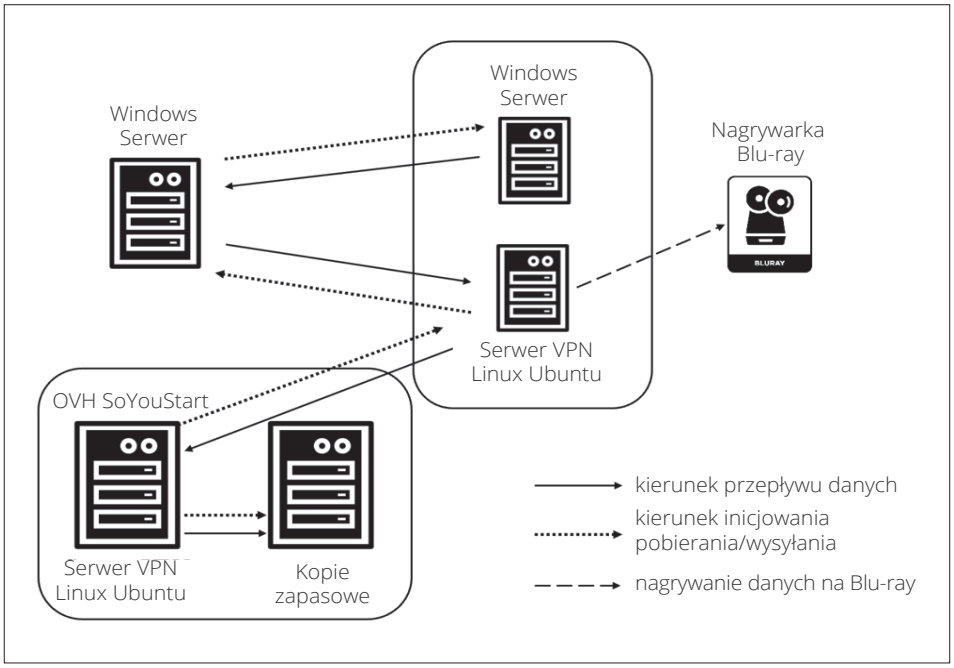
Obecnie na serwerze z VM znajdują się następujące serwery wirtualne (zob. rysunek 3):

- serwer z systemem Windows Server 2019, na którym znajdują się bazy danych programów firmy INSERT oraz programów przeznaczonych dla przedsiębiorstwa typu ERP;
- VPN – serwer pracujący pod kontrolą systemu Ubuntu Linux (16.04 LTS) – jest wykorzystywany jako koncentrator VPN oraz do przechowywania kopii danych baz danych z ostatniego tygodnia (w tym jako pośrednik przy przesyłaniu danych na serwer Cloud).

Na serwerze nie zainstalowano żadnego oprogramowania antywirusowego. Backup systemów skonfigurowany jest w ten sposób, że kopie składowane są na płytach Blu-ray oraz w tzw. chmurze. Na serwerach nie ma domeny, a użytkownicy mają założone konta lokalne w celu łączenia się *Remote Desktop Protocol* (RDP). Na serwerze został zainstalowany program *Insert GT*, z którego

korzystają użytkownicy, łącząc się RDP. Z zewnątrz połączenie odbywa się za pomocą *Open VPN*. W obecnej chwili serwer w jednym z budynków jest wyłączony, a zasoby są przeniesione na serwer z VM.

Rysunek 3. Schemat wykonywania kopii bezpieczeństwa – przepływ według kolejności



Źródło: opracowanie własne.

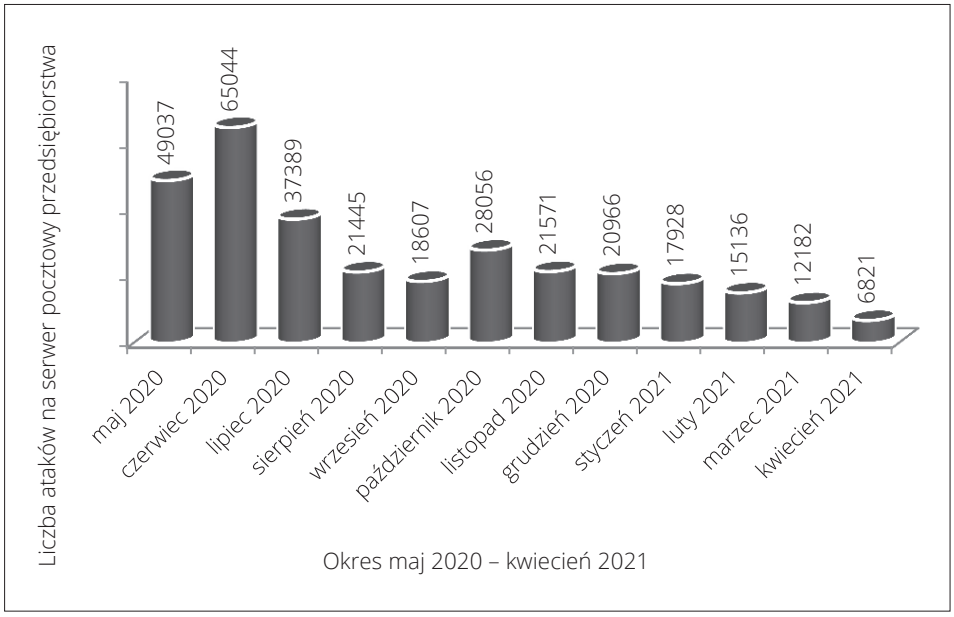
Ochrona serwerów pocztowych przed włamaniami, atakami destrukcyjnymi oraz wirusami

Serwery pocztowe są serwerami najczęściej narażonymi na ataki hakerskie[10]. W przypadku szybkiego włamania do serwera pocztowego można natychmiast utracić cenne dane kontrahentów oraz załączniki, które zawierają

[10] B.J. Koops, *Megatrends and grand challenges of cybercrime and cyberterrorism policy and research*, [w:] B. Akhgar, B. Brewster (red.), *Combatting Cybercrime and Cyberterrorism*, New York 2016, s. 3–15.

dane poufne transakcji finansowych[11]. Serwery pocztowe stają się miejscem dalszych działań hakerskich, polegających na próbie wyłudzenia danych od klientów przedsiębiorstwa, które podejmowało kontakt na wszystkie adresy mailowe istniejące w bazie[12]. Analizowane przedsiębiorstwo regularnie odnotowuje kilka tysięcy prób ataków zarówno na serwer pocztowy, jak i na własną witrynę internetową. W rekordowym miesiącu – czerwcu – 2020 r. odnotowano ponad 65 tys. ataków w ciągu jednego miesiąca (rysunek 4).

Rysunek 4. Liczba ataków na serwer pocztowy w analizowanym przedsiębiorstwie w okresie maj 2020 – kwiecień 2021



Źródło: opracowanie własne.

Zastosowanie zabezpieczeń w postaci plugginów w oprogramowaniu obsługującym serwer poczty wychodzącej oraz serwer poczty przychodzącej

[11] J.R. Jiang, *An improved cyber-physical systems architecture for Industry 4.0 smart factories*, „Advances in Mechanical Engineering" 2018, Vol. 10, No. 6, s. 1–15.

[12] D.C. Chou, D.C. Yen, B. Lin, P. Hong-Lam Cheng, *Cyberspace security management*, „Industrial Management Data Systems" 1999, Vol. 99, No. 8, s. 353–361.

i stały „ręczny" nadzór na ruchem serwerowym pozwoliły przedsiębiorstwu (po zatrudnieniu administratora danych serwera pocztowego) ograniczyć w sposób znaczny ataki hakerskie do kilku tysięcy miesięcznie. Wszystkie połączenia SMTP z Internetu są poddawane kontroli, a następnie są one zapisywane na dysku maszyny. Serwery poczty instytucji nie powinny być w ogóle osiągalne przez Internet[13].

Ochrona przed awariami realizowana jest poprzez tworzenie tzw. konfiguracji *High Availability* (HA). Firewall może funkcjonować w trzech konfiguracjach:

- *hot stand-by* – konfiguracja składa się z dwóch lub więcej maszyn firewall, wśród których tylko jedna jest aktywna, a pozostałe to maszyny zapasowe uruchamiane w razie awarii aktywnego firewalla (system zaporowy widoczny jest pod jednym adresem IP);
- *load sharing* – konfiguracja składa się z dwóch lub więcej maszyn firewall, spiętych w klaster, współdzielących ze sobą ruch sieci rozdzielany pomiędzy poszczególne firewalle przez urządzenia zewnętrzne, np. routery (w sieci widoczne są adresy IP poszczególnych maszyn firewall);
- *load balancing* – konfiguracja składa się z dwóch lub więcej maszyn firewall, spiętych w klaster, dynamicznie równoważących pomiędzy sobą obciążenie sieci (system zaporowy widoczny jest pod jednym adresem IP, wymaga zastosowania modułu *StoneBeat FullCluster*)[14].

Zabezpieczenie serwerów poczty przed awariami najczęściej odbywa się poprzez tworzenie wielu serwerów SMTP, obsługujących tę samą domenę poczty. Priorytet serwerów ustala się w DNS. W razie niedostępności serwera o najwyższym priorytecie poczta przesyłana jest do serwera o niższym priorytecie. Innym zagrożeniem dla prawidłowego funkcjonowania poczty internetowej jest niedostępność (np. zablokowanie, awaria) serwera DNS,

[13] J. Lee, B. Bagheri, H.A. Kao, *A cyber-physical systems architecture for Industry 4.0-based manufacturing systems*, „Manufacturing Letters" 2015, Vol. 3, s. 18–23.

[14] M. Stawowski, op. cit.

który udziela informacji na temat serwera poczty[15]. Zagrożenie wynika z tego, iż w wypadku, gdy adres IP serwera poczty określonej domeny nie zostanie znaleziony, przesyłki pocztowe wysyłane do tej domeny są odrzucane. Jest to bardziej groźne od awarii samego serwera poczty, ponieważ gdy serwer ten jest niedostępny, poczta do niego kierowana jest przechowywana przez długi czas na serwerze wysyłającym[16].

W typowej konfiguracji podstawowy serwer DNS, posiadający lokalną bazę danych dla swojej strefy DNS, instalowany jest w sieci chronionej przez firewall. Dodatkowy serwer DNS, nieposiadający stałej bazy danych, instalowany jest w sieci operatora Internetu. Serwer ten dla klientów DNS jest pełnowartościowym źródłem informacji. Dodatkowe serwery DNS odczytują dane na temat swoich stref z innych serwerów DNS.

Wirusy od wielu lat zajmują najwyższe miejsce na liście zagrożeń systemów komputerowych. W środowisku internetowym popularne stały się także inne groźne aplikacje: robaki (programy posiadające zdolności samodzielnego przenoszenia) i konie trojańskie (programy udające inne, legalne aplikacje). Skuteczny system ochrony przed tego typu zagrożeniami powinien opierać się na wielu warstwach zabezpieczeń. Najczęściej stosowana konfiguracja systemu ochrony przeciwwirusowej składa się z dwóch lub trzech warstw zlokalizowanych na firewallu, serwerach i stacjach użytkowników[17].

Powyższe dane zostały zebrane zgodnie z obowiązującymi przepisami prawa telekomunikacyjnego, art. 180a–180c, dotyczącymi obowiązku zatrzymywania, przechowywania, udostępniania i ochrony danych[18].

W przedsiębiorstwie stosuje się archiwizację błędnych logowań z danego adresu IP:

- błędne autoryzacje przy wysyłce poczty: 3 razy w ciągu 10 minut, następnie zostaje uruchomiona blokada na 30 minut,

[15] H.S. Chen, J. Fiscus, *The inhospitable vulnerability. A need for cybersecurity risk assessment in the hospitality industry,* „Journal of Hospitality and Tourism Technology" 2018, Vol. 9, No. 2, s. 223–234.

[16] M. Stawowski, op. cit.

[17] Ibidem.

[18] Art. 180a ustawy z dnia 16 lipca 2004 r., Prawo telekomunikacyjne (Dz.U.2020.0.576).

- błędne autoryzacje przy połączeniu POP3/IMAP (dotyczą odbierania poczty): 3 razy w ciągu 30 minut, później następuje blokada na 30 minut i 3 sekundy,
- błędne autoryzacje przy połączeniu FTP: 3 razy w ciągu 30 minut, później włączona zostaje blokada na 30 minut i 3 sekundy,
- dowolne próby logowania na strony (WordPress): 3 razy w ciągu 40 sekund, potem następuje blokada na 2 godziny,
- potrójne trafienie na blokadę w ciągu 24 godzin powoduje zablokowanie danego IP na 7 dni (to jest ta różnica widoczna od lipca 2020),
- w przypadku prób z wielu różnych adresów IP z danych zakresów i po sprawdzeniu logów różnych usług z okresu 2–3 miesięcy, czy były jakieś „pozytywne" zachowania (czy była dostarczona poczta albo były „standardowe wejścia na strony"), podejmowana jest decyzja o blokadzie danej puli adresowej na stałe / na dłuższy okres (np. 3–6 miesięcy),
- okresowe skany „wordpressów" w celu sprawdzenia, czy nie zawierają nieaktualnych/niebezpiecznych dodatków,
- *WebMail* – dodatkowo wprowadzona *captcha* – przy błędnych logowaniach aktywuje się opcja potwierdzenia (zabezpieczenie przy próbie ataków/zgadywania haseł do skrzynek przez automaty).

Zastosowano następujące działania w celu ograniczenia ataków na serwer pocztowy:

- filtry statyczne na podstawie znanych statycznych wpisów (nagłówki oraz treść wraz z załącznikami) – czyli aktualizowane na podstawie własnych obserwacji (w tym z innych serwerów czy własnych e-maili „pułapek"),
- filtrowanie na podstawie list RBL (z obsługą wyjątków),
- liczne ręczne sprawdzenia, czy:
  - serwer, który wysyła na serwer pocztę jest „poprawnie skonfigurowany",
  - posiada revDNS, czy domena istnieje,
  - docelowa domena istnieje u użytkownika,
- przekazywanie dodatkowych filtrów antyspam/antywirus.

Poszczególne warstwy ochrony powinny opierać się na technologiach różnych producentów[19].

Zalecenia dotyczące dalszych działań nad bezpieczeństwem danych serwerowych

Eksploatowane serwery przedsiębiorstwa są już po gwarancji, a więc każda awaria może wiązać się z długotrwałym brakiem dostępu do zasobów centralnych. Zalecono przedsiębiorcy wymianę sprzętu na nowy, objęty gwarancją producenta, albo, jeżeli to możliwe, wykupienie dodatkowej, przedłużonej gwarancji u producenta.

W celu zagwarantowania ciągłości pracy systemów serwerowych w razie awarii dobrym rozwiązaniem jest zbudowanie klastra na bazie np. dwóch identycznych serwerów fizycznych. Taka konfiguracja zapewni ciągłość pracy w przypadku awarii jednego z nich.

W przedsiębiorstwie należy ustalić aktualną listę niezbędnego oprogramowania potrzebnego do wykonywania pracy i zgodnie z nią przeprowadzić pełną kontrolę stacji roboczych. Programy, które nie są wymagane do wykonywania obowiązków służbowych, powinny zostać usunięte z komputerów służbowych.

Przedsiębiorstwo powinno przygotować plan inwestycji odnoszący się do wymiany stacji roboczych oraz zakupienia ich u jednego producenta. Umożliwia to wybranie odpowiedniej oferty, uzyskanie rabatów oraz bezproblemowe naprawy gwarancyjne.

Uzyskanie zadawalającego poziomu bezpieczeństwa danych procesowych w zasobach dostępnych z zewnątrz musi dotyczyć dwóch elementów:

1) Odpowiedniego zabezpieczenia haseł dostępu. Warunek ten można spełnić albo włączając serwer do domeny Windows (konieczność za-

[19] M. Alexander, *Methods for understanding and reducing social engineering attacks*, SANS Institute, www.sans.org/reading-room/whitepapers/critical/methods--understanding- reducing-social-engineering-attacks-36972 [dostęp: 8.04.2021].

stosowania serwera z odpowiednim oprogramowaniem), albo stosując wewnętrzną politykę bezpieczeństwa polegającą na częstej zmianie haseł i odpowiednim ich skomplikowaniu.

2) Zabezpieczenia transmisji internetowej. Dane w czasie transmisji przez publiczny Internet mogą zostać przechwycone przez programy szpiegujące. Dlatego dla ochrony przed tym zagrożeniem stosuje się mechanizmy ogólnie zwane VPN (Wirtualne Sieci Prywatne). Te mechanizmy wspierane przez odpowiednie routery szyfrują dane w czasie transmisji pomiędzy routerem zainstalowanym w firmie a komputerem znajdującym się w Internecie.

Oba te elementy stosowane wspólnie spowodują znaczący wzrost bezpieczeństwa danych. Należałoby na serwerze wdrożyć kontroler domeny. W celu ochrony danych przedsiębiorstwa zaleca się zakup dysków, na których zostaną wykonane bezpieczne kopie zapasowe wszystkich danych znajdujących się na serwerach.

BIBLIOGRAFIA

1. Alexander M., *Methods for understanding and reducing social engineering attacks*, SANS Institute, www.sans.org/reading-room/whitepapers/critical/methods-understanding-reducing-social-engineering-attacks-36972 [dostęp: 8.04.2021].
2. Bielawski K., Chmieliński M., Pabich M., *Zagrożenia bezpieczeństwa informacji oraz rozwiązania IT w zakresie wsparcia produkcji i logistyki w przedsiębiorstwie*, „Problems Mechatronics Armament, Aviation, Safety Engineering" 2017, t. 8, nr 4(30), s. 151–166.
3. Bilefsky D., *Hackers use new tactic at Austrian hotel: locking the doors*, „The New York Times", www.nytimes.com/2017/01/30/world/europe/hotel-austria-bitcoin-ransom.html?_r=0 [dostęp: 8.04.2021].
4. Bosman L., Hartman N., Sutherland J., *How manufacturing firm characteristics can influence decision making for investing in Industry 4.0 technologies*, „Journal of Manufacturing Technology Management" 2020, Vol. 31, No. 5, s. 117–114.

5. Cedeño J.M.V., Papinniemi J., Hannola L., Donoghue I., *Developing smart services by Internet of Things in manufacturing business*, „Lappeenranta University of Technology" 2018, Vol. 14(1), s. 59–71.
6. Chen H., *Applications of cyber-physical system: a literature review*, „Journal of Industrial Integration and Management" 2017, Vol. 2, No. 3, s. 1750012.
7. Chen H., *Theoretical foundations for cyber-physical systems: a literature review*, „Journal of Industrial Integration and Management" 2017, Vol. 2, No. 3, s. 1750013.
8. Chen H.S., Fiscus J., *The inhospitable vulnerability. A need for cybersecurity risk assessment in the hospitality industry,* „Journal of Hospitality and Tourism Technology" 2018, Vol. 9, No. 2, s. 223–234.
9. Chou D.C., Yen D.C., Lin B., Hong-Lam Cheng P., *Cyberspace security management*, „Industrial Management Data Systems" 1999, Vol. 99, No. 8, s. 353–361.
10. Jiang J.R., *An improved cyber-physical systems architecture for Industry 4.0 smart factories*, „Advances in Mechanical Engineering" 2018, Vol. 10, No. 6, s. 1–15.
11. Koops B.J., *Megatrends and grand challenges of cybercrime and cyberterrorism policy and research*, [w:] B. Akhgar, B. Brewster (red.), *Combatting Cybercrime and Cyberterrorism*, New York 2016, s. 3–15.
12. Lee J., Bagheri B., Kao H.A., *A cyber-physical systems architecture for Industry 4.0-based manufacturing systems*, „Manufacturing Letters" 2015, Vol. 3, s. 18–23.
13. Patkowski A., *„Cicha reakcja" na zdalne ataki teleinformatyczne*, „Przegląd Teleinformatyczny" 2017, t. 5, nr 3, s. 33–51.
14. Stawowski M., *Praktyczne metody ochrony poczty elektronicznej,* http://www.iniejawna.pl/pomoce/poczta.html [dostęp: 1.04.2021].
15. Tarabasz A., *Cybersecurity and Internet of threats – new challenges in customer behavior*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2018, nr 360, s. 64–81.