Cyberbezpieczeństwo i grzech zaniechania

Jak skutecznie zabezpieczyć się organizacyjnie i technologicznie przed cyberatakami? Jak oszacować ryzyko? Jak stworzyć bezpieczne Elektroniczne Miejsce Pracy? Na te i inne pytania odpowiada dr inż. Bożena Skibicka, pełnomocnik firmy informatycznej mis², prezes zarządu Stowarzyszenia Praktyków Zarządzania Wiedzą i wiceprzewodnicząca Konwentu Business Center Club.

Jakie są największe zagrożenia w obszarze cyberbezpieczeństwa w firmach produkcyjnych i co stanowi najsłabsze ogniwo?
W każdym przedsiębiorstwie – handlowym, usługowym i produkcyjnym – najsłabszym ogniwem jest człowiek. Niestety wielu menedżerów wciąż nie ma tej świadomości. Według dostępnych źródeł tylko 17 % wycieków danych spowodowanych jest obejściem zabezpieczeń infrastruktury teleinformatycznej. Pozostałe wynikają z błędów po stronie człowieka – jego braku świadomości, niefrasobliwości albo złej woli. Oczywiście łatwiej jest – mając odpowiedni budżet – zamówić i wdrożyć odpowiednie zabezpieczenia technologiczne niż budować w firmie kulturę bezpieczeństwa. Tymczasem tylko kompleksowe podejście – zabezpieczenie firmy przez zastosowanie odpowiednich, wzajemnie powiązanych rozwiązań informatycznych, prawnych, organizacyjnych oraz ubezpieczeniowych – może zmniejszyć ryzyko cyberataku i w konsekwencji utraty pieniędzy, a przede wszystkim zaufania obecnych i potencjalnych klientów.

Jakie incydenty bezpieczeństwa w sieciach przemysłowych mogą przynieść najgorsze konsekwencje?
Nie ma prostej odpowiedzi. Każdy incydent to zagrożenie ciągłości pro-

dukcji, ale też – w wyniku powiązania sieci OT i IT – utraty wizerunku marki, wspomnianego już zaufania obecnych i potencjalnych odbiorców oraz przychodów, a niekiedy konieczność poniesienia finansowych kar. Każde takie zdarzenie warto przeanalizować. Dostępne są publikacje opisujące, jakie kroki należy podjąć w reakcji na incydent (IR – Incident Response). Ponadto wszystkie firmy w dzisiejszych czasach powinny mieć opracowaną politykę bezpieczeństwa, uwzględniającą szereg dokumentów dotyczących cyberbezpieczeństwa, m.in. wspomnianego procesu IR.

Źródeł cyberataków może być wiele. Należą do nich brak technologicznych i technicznych zabezpieczeń systemów informatycznych oraz polityki ustawiania haseł i uprawnień do systemów informatycznych, nieaktualizowanie użytkowanego oprogramowania, niemonitorowanie bezpieczeństwa publicznie udostępnianych usług i korzystanie z dostępnego publicznie oprogramowania mającego podatność bezpieczeństwa. Kolejne to brak procedur prawnych i organizacyjnych przeciwdziałających niebezpieczeństwu oraz opracowanego i zatwierdzonego systemu zapewnienia ciągłości działania, a także brak kultury bezpieczeństwa zbudowanej w firmie i świadomości użytkowników o tym, skąd mogą płynąć zagrożenia oraz brak szkoleń.

Wyciek danych, ransomware, malware, ataki DDoS, pishing, botnety – które z tych zagrożeń jest największe i najgroźniejsze w skutkach?

Z punktu widzenia właściciela firmy czy menedżera nieważne są nazwy i to, co się pod nimi kryje. Ważna jest świadomość, że są to narzędzia stosowane w przemyśle przestępczym (crime industry), którego celem jest generowanie zysków naszym kosztem. Ta świadomość powinna prowadzić do budowania w każdej firmie polityki bezpieczeństwa cybernetycznego, w której docelowo na równi znajdą się rozwiązania organizacyjne, prawne oraz techniczno-informatyczne. Warto też oszacować ryzyko i pomyśleć o wykupieniu odpowiedniego ubezpieczenia – od dłuższego czasu takie ubezpieczenia są już dostępne na rynku.

W firmach produkcyjnych opracowanie polityki bezpieczeństwa cybernetycznego i wynikających z niej działań jest bardziej złożone niż w innych. Musi ona bowiem uwzględniać zabezpieczenie nie tylko sieci IT, ale również OT.

> POLITYKA BEZPIECZEŃSTWA TO ŻYWY DOKUMENT, KTÓRY MUSI BYĆ MODYFIKOWANY WRAZ Z POJAWIAJĄCYMI SIĘ NOWYMI ZAGROŻENIAMI LUB ZMIANAMI W SPOSOBIE FUNKCJONOWANIA FIRMY.

Czym ochrona tych pierwszych różni się od ochrony sieci przemysłowych?

W jednym i drugim przypadku kluczowe jest systemowe podejście. Nie zminimalizujemy ryzyka wycinkowymi działaniami i nawet najlepszymi zabezpieczeniami techniczno-informatycznymi – ani w sieci IT, ani w sieci OT. Potrzebna jest kompleksowa ochrona przed cyberatakami.

W przypadku sieci OT najistotniejsze jest zapewnienie bezpieczeństwa i niezawodności systemów sterowania. Trzeba przy tym pamiętać, że obie sieci przenikają się i są powiązane – nie tylko wewnętrznie, ale i zewnętrznie. Nie da się odgrodzić fabryki murem, postawić potężnego firewalla i w ten sposób zapewnić fabryce bezpieczeństwo. Musimy wciąż badać podatność urządzeń oraz aplikacji na włamania i edukować siebie oraz naszych pracowników w tym obszarze. Jak mantrę będę powtarzać, że kluczowe jest systemowe podejście do cyberbezpieczeństwa i cząstkowe rozwiązania nie zapewnią nam spokojnego snu.

Rośnie w siłę infrastruktura biznesowa cyberprzestępców, której elementem jest podziemny rynek usług hostingowych i pokrewnych, np. hostingu zabezpieczonego przed organami ścigania – bulletproof hosting, wirtualnych sieci VPN, serwerów anonimizujących i zabezpieczeń przed atakami typu DDoS. Część osób uważa, że wymienione zagrożenia dotyczą przede wszystkim osób prywatnych i firm, a nie samej produkcji. Jakie jest Pani zdanie?

Produkcja w Przemyśle 4.0 oparta jest w dużej mierze na IIoT (Przemysłowy Internet Rzeczy) i cloud computing, a więc ta powszechna i nieprawdziwa opinia wynika po prostu z braku wiedzy.

Internet Rzeczy i Przemysłowy Internet Rzeczy – inteligentne czujniki, systemy sterujące itp. – są coraz bardziej obecne w świecie przemysłu, ale nie jest jeszcze powszechny, zwłaszcza w mniejszych firmach. Na ile barierą do szybszego jego upowszechnienia jest obawa o cyberbezpieczeństwo i brak wdrożonych w tym zakresie działań?

Uważam, że to nie obawa o bezpieczeństwo w większości przypadków jest barierą, ale raczej brak wiedzy, jak wprowadzać rozwiązania cyfrowe. Zastrzegam przy tym, że mówimy o rynku MŚP, bo dla dużych, międzynarodowych korporacji sieci Przemysłu 4.0 są już rzeczywistością. W MŚP to dla niektórych początek, a dla większości przyszłość. Warto zwrócić uwagę na fakt, że funkcjonujemy w globalnej gospodarce. Chcąc być konkurencyjnym, nie da się dzisiaj zamknąć na jednym rynku. To złożone zagadnienie i temat na osobną rozmowę. Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji na swoim tegorocznym, 13. Forum Gospodarczym TIME, które odbędzie się w formule on-line w dniach 8–11 marca 2021 r., przybliży temat Przemysłu 4.0 właśnie w kategoriach sieciowych. Jeśli kogoś z Czytelników interesuje ten temat, będzie okazja, by go wtedy zgłębić.

Fot. mis²

Jako jedna z barier poprawy cyberbepieczeństwa wymieniane są koszty takich zabezpieczeń. Na ile Pani zdaniem jest to kwestia czysto obiektywna, tj. brak wystarczających środków na takie inwestycje, a na ile kwestia podejścia zakładającego, że lepiej inwestować w inne działania i bagatelizowanie potencjalnych zagrożeń?

Ciekawe byłyby badania pozwalające odpowiedzieć na pytanie, ile firm produkcyjnych wykonało audyt w obszarze potencjalnych zagrożeń, oszacowało koszty i sformułowało zalecenia dotyczące zabezpieczeń.

Inwestycje w tym obszarze są zależne od oceny ryzyka, jakie niesie ze sobą ewentualny cyberatak. Trzeba zidentyfikować czynniki, które mogą być źródłem ataku i spowodować szkodę, a następnie przypisać tym szkodom konsekwencje finansowe i zdecydować, czy stać nas na takie ryzyko.

Często nie badamy się systematycznie, bo myślimy, że nie zachorujemy. W przypadku cyberataków jest podobnie. Tymczasem gdy popatrzymy na skalę zjawiska, powinniśmy zacząć się bać. Według opublikowanego kilka dni temu raportu firmy Xopero na początku 2016 r. tylko ransomware uderzał co dwie minuty, zaś rok później co 40 sekund. W 2019 r. było to już 14 sekund, a w 2021 r. ten czas ma się skrócić do 11 sekund! Według tego samego raportu, który powołuje się na Cybersecurity Ventures, wartość globalnych szkód powstałych za sprawą ransomware szacowana jest w 2021 r. na kwotę 20 mld dolarów.

Ataki nie omijają Polski. Z badania ankietowego przeprowadzonego przez Business Center Club pod koniec czerwca 2019 r. wynika, że 61,76 % respondentów doświadczyło ataku hakerskiego.

Najczęściej ofiarą cyberataków padają nie wielkie korporacje, tylko MŚP (41 % wszystkich ataków). Jednocześnie z danych przedstawionych przez PricewaterhouseCoopers wynika, że tylko 50 % wszystkich przedsiębiorstw jest właściwie przygotowana do walki z cyberatakami.

Cyberataki zaczynają być znacznie bardziej dochodowe niż biznes narkotykowy – rozmiary cyberprzestępczości porównywalne są obecnie z wartością całego rynku narkotykowego i szacowane są na prawie 400 mld dolarów łącznie. Dlatego warto przeanalizować koszty wynikające z potencjalnego ataku. Zaliczamy do nich koszty związane ze śledztwem informatycznym, poinformowaniem potencjalnych poszkodowanych, działaniami PR dla powstrzymania procesu utraty dobrego imienia, a w konsekwencji zaufania klientów na skutek wycieku danych, a ponadto koszty związane z obroną prawną, odszkodowaniami, karami administracyjnymi, karami ustawowymi związanymi z RODO (4 % przychodów), usługami ekspertów i ekspertyzami oraz okupem dla szantażysty. Musimy też pamiętać o odpowiedzialności cywilnej i administracyjnej firmy i osób zarządzających.

Każda firma i każdy zarządzający musi zastanowić się i przeliczyć ryzyko poniesienia tych kosztów w odniesieniu do kosztów inwestycji w stworzenie polityki bezpieczeństwa w firmie i wdrożenie odpowiednich, wzajemnie ze sobą powiązanych rozwiązań informatycznych, prawnych, organizacyjnych oraz ubezpieczeniowych. Uważam, że tylko takie kompleksowe podejście minimalizuje ryzyko, a w razie cyberataku przenosi finansowe konsekwencje poza firmę, tj. na towarzystwa ubezpieczeń.

Rozumiejąc kwestie budowania bezpieczeństwa cybernetycznego firm całościowo, powołaliśmy Konsorcjum na rzecz Cyberbezpieczeństwa, w skład którego wchodzi firma informatyczna mis^2, Kancelaria Prawa Sportowego i Gospodarczego Dauerman oraz Broker Ubezpieczeniowy i Reasekuracyjny Konstanta PWS. Przeprowadzamy audyt prawny i informatyczny, formułujemy zalecenia oraz proponujemy zainteresowanym odpowiednią polisę ubezpieczeniową.

Jakie są najczęstsze błędy we wdrażaniu i realizacji założeń cyberbezpieczeństwa?

Zawsze najczęstszym błędem jest zaniechanie. Wszystkie zalecenia wynikające ze zrealizowanych audytów należy wdrożyć, a następnie cyklicznie przeprowadzać kolejne audyty, sprawdzać podatność oprogramowania i urządzeń oraz ustawicznie szkolić pracowników. W konsekwencji stworzymy w firmie kulturę bezpieczeństwa cybernetycznego, gdzie wszyscy pracownicy oraz podwykonawcy, nawet firmy sprzątające, są świadomymi użytkownikami naszej sieci oraz wewnętrznych uregu-

BOŻENA SKIBICKA

Fot. mis^2

Pełnomocnik spółki mis^2, prezes zarządu Stowarzyszenia Praktyków Zarządzania Wiedzą, wiceprzewodnicząca Konwentu Business Center Club. Przedstawicielka Loży Dolnośląskiej Business Center Club w Komitecie Monitorującym RPO Województwa Dolnośląskiego 2014–2020 oraz członek Rady Doradców Kanclerza Loży Dolnośląskiej BCC.

Z branżą informatyczną związana od 1990 r. Jej specjalizacja to zarządzanie dokumentami i automatyzacja procesów, analityka biznesowa oraz cyberbezpieczeństwo. Autorka licznych publikacji z tego zakresu. Prowadziła wiele projektów wdrożeniowych o różnej skali, zarówno w sektorze publicznym, jak i komercyjnym. W ramach różnych organizacji bardzo aktywnie działa na rzecz propagowania wśród firm sektora MŚP nowoczesnych narzędzi informatycznych.

Doktor nauk ekonomicznych. Ukończyła Politechnikę Wrocławską oraz staże naukowe na Uniwersytecie w Tsukubie (Japonia) i Uniwersytecie w Mariborze (Słowenia). W wolnym czasie gra w golfa.

lowań prawnych związanych z ochroną tajemnicy przedsiębiorstwa i użytkowaniem zarówno sieci IT, jak i OT.

Warto podkreślić, że dzisiaj wiele działań z tego zakresu można zoptymalizować, np. dzięki szkoleniom dla pracowników organizowanym on-line. Skanowanie urządzeń, oprogramowania, stron internetowych można powierzyć wyspecjalizowanym firmom, które będą to robić cyklicznie i na bieżąco informować o powstałych zagrożeniach.

Na czym powinna opierać się kompleksowa strategia cyberbezpieczeństwa? Na co należy zwrócić największą uwagę przy jej tworzeniu, a następnie realizacji?

Podstawą budowania kompleksowej strategii cyberbezpieczeństwa jest zrozumienie, jak funkcjonuje nasza firma, zidentyfikowanie wszystkich zachodzących w niej procesów i ocena, które z nich są krytyczne dla jej prawidłowego funkcjonowania. Jeśli mamy taką wiedzę, możemy przystąpić do oceny wrażliwości tych procesów na cyberzagrożenia.

Kolejny krok to ocena potencjalnych strat wywołanych przez udane cyberataki. Mając te wszystkie dane, możemy zdefiniować i wycenić, ile będzie nas kosztować zminimalizowanie zagrożeń. Środki wykorzystywane do ich minimalizacji to nie tylko narzędzia informatyczne, to przede wszystkim procedury wewnętrzne, szkolenia pracowników, ciągłe uświadamianie potencjalnych zagrożeń i monitorowanie skuteczności zabezpieczeń. Wszystko to składa się na politykę bezpieczeństwa, która w formie uzgodnionego i powszechnie znanego dokumentu powinna funkcjonować w każdej firmie. Polityka bezpieczeństwa to żywy dokument, który musi być modyfikowany wraz z pojawiającymi się nowymi zagrożeniami lub zmianami w sposobie funkcjonowania firmy.

Niezwykle istotnym elementem budowania strategii bezpieczeństwa jest wybór środków ochrony firmy przed zagrożeniami. Porównując potencjalne straty wynikające z naruszeń bezpieczeństwa z kosztami zabezpieczenia, musimy podjąć decyzję, jakie zastosować środki. W sytuacji, kiedy prawdopodobieństwo zagrożenia jest niewielkie, a potencjalne straty małe, inwestowanie w kosztowne zabezpieczenia nie musi być celowe. Należy jednak podkreślić, że takie decyzje muszą być podejmowane świadomie, z dogłębną wiedzą o warunkach występowania zagrożeń i ich skutkach.

Jakie największe wyzwania stoją dziś przez zakładami przemysłowymi w odniesieniu do zapewnienia cyberbezpieczeństwa?

Dzisiaj największym wyzwaniem stojącym przed firmami produkcyjnymi jest transformacja Przemysł 4.0, której celem jest przygotowanie zakładu do uczestnictwa w zintegrowanym cyfrowo systemie produkcji globalnej. Jak już wspomniałam wcześniej, to temat bardzo złożony, na osobną rozmowę. Przygotowując się do takiej transformacji, tym bardziej powinniśmy już dzisiaj zadbać o bezpieczeństwo cyfrowe, podchodząc do zagadnienia kompleksowo i kładąc duży nacisk na rozwiązania prawne i organizacyjne.

Czy można wskazać, które sektory przemysłu są najbardziej narażone na cyberataki i w których z nich takie ataki mogą przynieść najgroźniejsze skutki?

Dzisiaj każde przedsiębiorstwo w każdej branży, które posiada wartościowe dane, jest narażone na atak. Według raportu State of Ransomware 2020 – Niezależnego badania 5000 managerów IT w 26 krajach, zleconego przez firmę Sophos i przeprowadzonego przez firmę Vanson Bourne – ponad połowa ankietowanych firm (51 %) przyznała, że w minionym roku doświadczyła ataku ransomware. Najczęściej atakowane były firmy z grupy Media, rekreacja, rozrywka – 60 % ankietowanych firm z tego sektora doświadczyło takich ataków. Kolejna grupa to IT, technologia, telekomunikacja – 56 % i grupa Energia, ropa naftowa/gaz, firmy komunalne – 55 %.

Cyberprzestępcy wybierają firmy, które w swoich zasobach mają dane o wartości rynkowej, jak dane osobowe, numery kart kredytowych i dane wrażliwe, a także firmy, dla których zatrzymanie procesów produkcyjnych wiąże się z wielkimi stratami. W pierwszym przypadku przestępcy pozyskują dane, którymi mogą handlować, a w drugim przypadku firmy są skłonne do zapłacenia okupu, aby zminimalizować straty wynikające z zakłócenia lub zatrzymania procesów produkcyjnych. Niezwykle istotnym aspektem rozważanym przy wyborze celu ataku jest kwestia zaufania klientów do danej firmy. Przykładem może być ujawnienie braku wystarczającego zabezpieczenia danych klienta w banku, które stanowi istotny uszczerbek reputacji i z pewnością nie zachęca klientów do zakładania i utrzymywania konta w takim banku. Stąd zapewne bierze się widoczna powściągliwość kierownictwa poszkodowanej firmy w ujawnianiu faktu cyberataku, w szczególności udanego.

Czy Pani zdaniem do poprawy cyberpezpieczeństwa mogłyby przyczynić się ujednolicone, międzynarodowe standardy i certyfikaty bezpieczeństwa?

Oczywiście. Tak jak firmy podnoszą swoją wiarygodność w oczach kontrahentów przez certyfikację ISO 2000 czy ISO 27001, tak dzisiaj powinniśmy wypromować normy związane z cyberbezpieczeństwem i nawiązując współpracę sprawdzać, czy potencjalny kontrahent spełnia zalecane standardy.

Na świecie przeciwwagą dla ryzyka są działania prewencyjne. Warto powszechnie rozwijać takie podejście wśród naszych przedsiębiorców. Warto też znać obowiązujące w Polsce normy z obszaru bezpieczeństwa informatycznego, które są systematycznie aktualizowane.

Czy zainteresowanie usługami zapewnienia bezpieczeństwa infrastruktury informatycznej w Polsce rośnie?

Wydaje się, że rośnie popularność usług w obszarze sprzedaży oprogramowania zabezpieczającego. Nie widzę natomiast wzrostu zainteresowania kompleksowym podejściem. Zainteresowanie cyberryzykiem i kompleksowym zabezpieczeniem ze strony przedsiębiorców narasta powoli – niestety wolniej niż „rozwija się" ryzyko.

Obowiązujące w Polsce normy z obszaru bezpieczeństwa informatycznego (w lipcu i wrześniu 2020 r. ukazały się aktualizacje Polskich Norm z przedmiotowego zakresu):

- PN-EN ISO/IEC 15408-1:2020-09E Technika informatyczna – Techniki zabezpieczeń – Kryteria oceny zabezpieczeń informatycznych – Część 1: Wprowadzenie i model ogólny,
- PN-EN ISO/IEC 15408-2:2020-09E (...) Część 2: Komponenty funkcjonalne zabezpieczeń,
- PN-EN ISO/IEC 15408-3:2020-09E (...) Część 3: Komponenty uzasadnienia zaufania do zabezpieczeń,
- PN-EN ISO/IEC 18045:2020-09E Technika informatyczna – Techniki bezpieczeństwa – Metodyka oceny zabezpieczeń informatycznych,
- PN-EN ISO/IEC 27000:2020-07E Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Przegląd i terminologia,
- PN-EN ISO/IEC 27019:2020-09E Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie bezpieczeństwem informacji w branży energetycznej,
- PN-EN ISO/IEC 29134:2020-09E Technika informatyczna – Techniki bezpieczeństwa – Wytyczne dotyczące oceny skutków dla prywatności,
- PN-ISO/IEC 29151:2019-01P Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady ochrony informacji o identyfikowalnych osobach,
- PN-ISO/IEC 29100:2017-07/A1:2019-09E Technika informatyczna – Techniki bezpieczeństwa – Ramy prywatności,
- Międzynarodowe standardy – ISO / IEC 27001 i 27002, ISO 15408.

COVID-19 i rozwinięcie na powszechną skalę pracy zdalnej, w ramach której duża część komunikacji odbywa się przez komunikatory, webinary, wideokonferencje, zaowocował zwiększeniem ryzyka w obszarze cyberbezpieczeństwa i ochrony danych. Jak sobie z tym radzimy Pani zdaniem?
Myślę, że dzisiaj większość przedsiębiorców i zarządów firm jest już przekonanych, że takie zorganizowanie pracy, by większość procesów biznesowych mogła przebiegać w formie elektronicznej, jest konieczne.

Ogólnoświatowa epidemia przyśpieszyła cyfryzację naszych przedsiębiorstw o co najmniej dekadę, przy czym w bardzo wielu firmach, szczególnie z sektora MŚP, wciąż nie pracujemy w pełni zdalnie, raczej w trybie home office. Często nie mamy bowiem dostępu on-line do potrzebnych dokumentów. Musimy prosić innych o ich przesłanie pocztą elektroniczną albo pojechać po nie do biura. Nie trzeba chyba tłumaczyć, jak niebezpieczne jest wysyłanie ważnych dokumentów pocztą elektroniczną bez odpowiednich zabezpieczeń. Można oczywiście rozwiązać ten problem, wprowadzając odpowiednie reguły opisujące bezpieczny sposób ich przesyłania tą drogą. Jednak uważam, ze znacznie bezpieczniejsze jest wdrożenie pracy zdalnej, a to wymaga stworzenia dla każdego pracownika Elektronicznego Miejsca Pracy. Elektroniczne Miejsce Pracy to elektroniczne biurko, tyle, że nie w tradycyjnym biurze, a w biurze, które zostało przeniesione na elektroniczną platformę. Na niej pracownik znajduje wszystko, co jest mu potrzebne do pracy, a ponadto może łatwo komunikować się z zarządem, innymi pracownikami oraz światem zewnętrznym. Bardziej zaawansowane platformy zawierają dodatkowo wpisane w nie zautomatyzowane procesy biznesowe. Jest to połączenie systemu obiegu dokumentów, dostępu do zautomatyzowanych procesów oraz narzędzi komunikacji.

Po zalogowaniu się do Elektronicznego Miejsca Pracy pracownik ma wszystkie niezbędne informacje w jednym miejscu, wraz z możliwością komunikacji, współpracy i wymiany wiedzy z innymi członkami zespołu oraz otoczeniem. Nie musi logować się do kolejnych aplikacji, przeszukiwać skrzynki elektronicznej – wszystko jest w EMP, począwszy od korespondencji z klientami, wewnętrznych zarządzeń i wzorów potrzebnych dokumentów, po możliwość wystawienia delegacji czy sprawdzenia przysługującej liczby dni urlopowych. Oczywiście każdy pracownik ma dostęp tylko do tych dokumentów i funkcjonalności, do których powinien mieć uprawnienia. Co bardzo ważne – niczego nie musimy szukać w skrzynce mailowej, bez pewności, czy to, co znajdziemy jest ostatnią wersją poszukiwanego dokumentu. Bardzo istotnym elementem EMP jest bowiem wyeliminowanie maili z korespondencji wewnętrznej. Skrzynka pocztowa służy do przyjmowania korespondencji mailowej z zewnątrz. Pracownicy i współpracownicy w ramach tej samej organizacji posługują się wewnętrznym systemem komunikacji, zwanym powiadomieniami.

Utrzymywanie dokumentów w zabezpieczonym przed nieupoważnionym dostępem repozytorium z mechanizmami bezpiecznego dostępu pozwala na znaczące zminimalizowanie zagrożenia udostępnienia istotnych z punktu widzenia firmy informacji i danych nieuprawnionym osobom. Trzeba przy tym podkreślić, że zabezpieczenie to obejmuje również pracowników firmy, bo przecież nie wszyscy powinni mieć dostęp do wszystkich dokumentów. W przeciwieństwie do poczty elektronicznej możemy w takim rozwiązaniu monitorować wykorzystanie dokumentów i kontrolować, kto i kiedy miał do nich dostęp.

Oczywiście tak jak i wcześniej, dbając o bezpieczeństwo cyfrowe, musimy zapewnić odpowiednie urządzenia, programy, organizację oraz rozwiązania prawne.

Rozmawiała
Urszula Chojnacka
AUTOMATYKA