Warszawa, 5 października 2022 r.

Komentarz

**Cyberbezpieczeństwo to technologie, ludzie i procesy**

**- Dziś firmy specjalistów ds. cyberbezpieczeństwa widzą w ekspertach od analizy złośliwego oprogramowania, obsługi SIEM czy forensic, ale nie w menedżerach, którzy potrafią patrzeć na cyberbezpieczeństwo we wspomniany już holistyczny sposób i widzą zależności pomiędzy ludźmi, technologiami i procesami. Rola takich menedżerów nie jest dziś jeszcze dobrze rozumiana, ale ich deficyt na rynku będzie widoczny i odczuwalny – prognozują w wywiadzie dr hab. Krzysztof Szczypiorski, profesor Politechniki Warszawskiej, Członek Zarządu Fundacji Bezpieczna Cyberprzestrzeń i Mirosław Maj, Prezes Fundacji Bezpieczna Cyberprzestrzeń - wykładowcy w Szkole Biznesu Politechniki Warszawskiej.**

**Z czego wynika wzrost popytu na specjalistów zajmujących się cyberbezpieczeństwem? Jak rynek ich dziś pozyskuje?**

**Mirosław Maj:** Zapotrzebowanie na kompetencje związane z cyberbezpieczeństwem rośnie naturalnie wraz z cyfrową transformacją i wzrostem zużycia systemów IT. Wzrosło też użycie systemów IT w kontekście wykorzystywania ich do tzw. krytycznych form działalności, związanych z ekonomią czy bezpieczeństwem również na poziomie kraju, co oznacza, że potrzeba coraz więcej ludzi i coraz więcej kompetencji do ich obsługi. Idąc jednak od samej genezy problemu – a więc powstania Internetu w latach 60. – wiemy, że nie został on zaprojektowany w bezpieczny sposób, a protokoły, które zostały wtedy wymyślone, w dużej mierze funkcjonują do dziś. Nie miały one natywnie zaimplementowanych funkcji bezpieczeństwa. Rośnie zapotrzebowanie na specjalistów od cyberbezpieczeństwa i na to, by ktoś potrafił nad tym zapanować – dzisiaj już w znacznie bardziej skomplikowanej materii jaką przez ponad pół wieku stała się sieć internetowa i świadczone w niej usługi.

Wzrost zapotrzebowania na ekspertów od cyberbezpieczeństwa stanowi poważne wyzwanie dla biznesu. Warto bowiem zaznaczyć, że branża IT nie ma niestety łatwo skalowalnego modelu, w którym mogłaby kształcić zawodowo jeden za drugim ekspertów od cyberbezpieczeństwa. Takich specjalistów nie można szkolić „taśmowo”, jednego za drugim i według jednego standardu tak, jak na przykład można szkolić – dajmy na to - operatorów dronów. „Cyberbezpieczeństwo” to pojemne pojęcie, na które składa się mnóstwo wąskich specjalizacji, związanych tak z rozumieniem technologii, jak i zarządzaniem procesowym. Zapotrzebowanie na cyberekspertów jest duże, ale mówimy o popycie na pracowników o bardzo niszowym, wąskim obszarze specjalizacji.

**Krzysztof Szczypiorski:** Rynek w końcu dojrzał i docenił cyberbezpieczeństwo, mimo że przez długi czas niechętnie płacił za specjalizację w tym kierunku. Z jednej strony z różnych względów przyspieszyła cyfryzacja biznesu, a z drugiej – w ostatnich latach doszło do wielu spektakularnych ataków, które uświadomiły raczej wszystkim, jak łatwo można przechwycić informacje i je spieniężyć. Dziś zapotrzebowanie na specjalistów ds. cyberbezpieczeństwa jest ogromne, a rynek cały czas wywiera presję, aby kształciło się ich coraz więcej. Choć nie brakuje genialnych samouków, to spora część tych osób wymaga dodatkowej edukacji i uzupełnienia wiedzy. Z drugiej strony brakuje kadr dydaktycznych – widać choćby deficyt ekspertów, którzy chcieliby i mogliby uczyć przyszłych specjalistów.

**Co składa się na rozwój cyberbezpieczeństwa w organizacji? Rozwój kompetencji pracowników, kadry zarządzającej… i co jeszcze? Na co powinny „iść” wydatki na cyberbezpieczeństwo?**

**Mirosław Maj:** Zanim odpowiem, ustalmy kluczową kwestię – rozwój cyberbezpieczeństwa nie jest kosztem czy jednorazowym wydatkiem. Jest inwestycją taką samą, jak zakup sprzętu IT. Ktoś, kto kupuje infrastrukturę informatyczną w ramach wielomilionowych budżetów, nie mówi z perspektywy lat, że poniósł koszt czy wydatek na jej zakup. Zawsze będzie podkreślał, że dokonał inwestycji. Takie samo myślenie powinno towarzyszyć cyberbezpieczeństwu. Co ważne – nie zawsze taka inwestycja wymaga gigantycznych nakładów finansowych. W cyberbezpieczeństwo można i trzeba inwestować rozsądnie i optymalnie.

Wracając jednak do pytania – chcemy, by spojrzenie na ten obszar było holistyczne i obejmowało trzy jego główne komponenty: technologie, ludzi i procesy. Wszystkie wymagają inwestowania. Posłużę się zresztą dosyć praktycznym i żywym przykładem: Jednym ze sztandarowych miejsc, o których się mówi w kontekście cyberbezpieczeństwa, są tzw. SOC-i (Security Operation Center). Parę lat temu nasilił się negatywny trend, polegający na tym, że SOC-i były budowane głównie prawie tylko w oparciu o SIEM-y, czyli główne urządzenia obsługujące centra bezpieczeństwa. Doszło wręcz do tego, dla większości firm i organizacji zbudowanie SOC było tożsame wyłącznie z zakupem SIEM. To zaczęło nagminnie doprowadzać do sytuacji, w której SIEM-y generowały komunikaty, których…. Nie rozumiał nikt w organizacji. A nawet gdy wiedział, co oznaczają, w organizacji nie było klarownych zasad definiujących, jak się zachować i jakie procedury należy wdrożyć w przypadku danego incydentu.

Wszystkie te trzy komponenty – ludzie, procesy i technologie – są zatem nieodzowne i w każdy z nich trzeba inwestować. W cyberbezpieczeństwie ludzie i technologie nie mogą funkcjonować prawidłowo bez zdefiniowanych procesów, technologie i procesy nie będą mogły zostać optymalnie wykorzystane bez ludzi, a ludzie i procesy potrzebują odpowiednich technologii.

**Jak przekonać kadrę zarządzającą do inwestycji w cyberbezpieczeństwo albo konkretnie w rozwój kompetencji powiązanych z cyberbezpieczeństwem? Jakich argumentów należy użyć?**

**Krzysztof Szczypiorski**: Gdybym miał przekonywać zarząd, użyłbym argumentu o ciągłości działania przedsiębiorstwa i o tym, że incydenty związane z cyberbezpieczeństwem zaburzają taką ciągłość. Taka argumentacja jest uniwersalna i pasuje do każdego profilu działalności.

**Mirosław Maj**: Znam dwie metody. Jedna jest dosyć brutalna i skrajna i nie do końca się z nią zgadzam, ale niestety, nie można odmówić jej przynajmniej częściowej efektywności. Widać bowiem, że najczęściej potrafi skłonić kadrę zarządzającą do podjęcia decyzji o inwestycji w cyberbezpieczeństwo. Tą metodą jest „przestraszenie” – a więc po prostu poczekanie, aż dojdzie do incydentu naruszającego cyberbezpieczeństwo. Warto przytoczyć tu historię jednego z czołowych polskich graczy na rynku e-commerce, który kilka lat temu zmagał się z systematycznymi atakami klasy DDoS, prowadzącymi do blokady usług internetowych (a więc zamknięcia serwisów). Straty wynikające z ataków sięgały miliony złotych dziennie i po prostu w pewnym momencie uznano, że wielomilionowa inwestycja w cyberbezpieczeństwo będzie dotkliwa, ale pomoże zapobiec podobnym incydentom w przyszłości. Taki „straszak” może być jednak skuteczny tylko na krótką metę – przedsiębiorca jest bardziej świadomy i wyczulony na punkcie cyberbezpieczeństwa tylko na czas ataku, zaś gdy zagrożenie minie, traci motywację do długiej inwestycji i nie wydaje się mu ona nieodzowna.

Druga metoda jest mi zdecydowanie bliższa, choć trudniejsza i wymaga długotrwałych działań. Polega na mówieniu o korzyściach językiem biznesu i twardymi danymi. Na przykład na oszacowaniu wartości firmy, jej mocy produkcyjnych i ocenie, o ile produkcja mogłaby zmaleć, gdyby doszło do incydentu związanego z cyberbezpieczeństwem. Możemy przecież powiedzieć zarządowi: „W porządku, możemy nie inwestować w cyberbezpieczeństwo, ale jeśli tego nie zrobimy, to w przypadku cyberataku dojdzie do poważnego zakłócenia procesów, przez który powrót do optymalnej wydajności zakładu zajmie nam minimum 3 dni.” Wystarczy wówczas sprawdzić w księgowości, jakie to są koszty i ile firma może stracić na takim potencjalnym przestoju. To bardziej wymagająca argumentacja, ale w mojej ocenie ma mocniejsze, stabilniejsze fundamenty i pozwala na to, że cyberbezpieczeństwo na stale zagości w budżetach inwestycyjnych.

**Kogo należy szkolić? Menedżerów, specjalistów IT?**

**Mirosław Maj:** Specjalistów brakuje niemal na każdym polu już dziś, ale istnieją ciekawe prognozy, z których wynika, że w niedalekiej przyszłości wzrośnie przede wszystkim krzywa zapotrzebowania na osoby specjalizujące się w sprawnym zarządzaniu cyberbezpieczeństwem. Dziś firmy ekspertów widzą w specjalistach od analizy złośliwego oprogramowania, obsługi SIEM czy forensic, ale nie w menedżerach, którzy potrafią patrzeć na cyberbezpieczeństwo we wspomniany już holistyczny sposób i widzą zależności pomiędzy ludźmi, technologiami i procesami. Rola takich menedżerów nie jest dziś jeszcze dobrze rozumiana, ale ich deficyt na rynku będzie widoczny i odczuwalny. To właśnie takich specjalistów chcemy szkolić w Szkole Biznesu Politechniki Warszawskiej na programie MBA Cybersecurity Management.

**Krzysztof Szczypiorski:** Uważam, że powinno się kształcić wszystkich w danej organizacji, czy też w firmie. Nie można uczyć zasad ruchu drogowego tylko części użytkowników, np. pominąć rowerzystów i motocyklistów tylko dlatego, że ci jeżdżą na dwóch kołach. Każdy uczestnik cyfrowego świata powinien w mniejszym lub większym stopniu być świadomy zagrożeń i umieć sobie z nimi radzić. Nawet pracownicy, którzy w swojej pracy nie zajmują się cyberbezpieczeństwem, powinni być obyci z tzw. cyfrową higieną, być odporni na ataki phishingowe, wiedzieć, jakie zagrożenia mogą czyhać podczas przeglądania skrzynki mailowej. Jeśli nie – powinni być szkoleni i uświadamiani. Nie ma w tej kwestii wyjątków.

Oczywiście, w dużych organizacjach powinna istnieć grupa osób, która – tak jak wskazał mój przedmówca - zarządza cyberbezpieczeństwem i jest odpowiedzialna za to, by firma mogła funkcjonować bezpiecznie.

**Mirosław Maj**

Założyciel i prezes Fundacji Bezpieczna Cyberprzestrzeń, wiceprezes spółki ComCERT SA. W latach 2017-2018 był doradcą Ministra Obrony Narodowej. Wcześniej związany z NASK, gdzie kierował zespołem CERT Polska. Był członkiem stałego zespołu ds. cyberbezpieczeństwa RP powołanego przez szefa BBN, brał udział w tworzeniu ustawy o Krajowym Systemie Cyberbezpieczeństwa. Zasiada w Radzie do spraw Cyfryzacji.

**Dr hab. inż. Krzysztof Szczypiorski, prof. PW**

Profesor Politechniki Warszawskiej. Kierownik i współtwórca Zakładu Cyberbezpieczeństwa w Instytucie Telekomunikacji (IT) na Wydziale Elektroniki i Technik Informacyjnych (WEiTI) Politechniki Warszawskiej (PW). Współtwórca i kierownik Centrum Badawczego POB Cyberbezpieczeństwo i Analiza Danych na PW. Kierownik kierunku kształcenia cyberbezpieczeństwo na WEiTI PW. Kierownik studiów podyplomowych MBA Cybersecurity Management w Szkole Biznesu Politechniki Warszawskiej.

**O Szkole Biznesu Politechniki Warszawskiej**

Szkoła Biznesu PW powstała w 1991 roku jako wynik wspólnego przedsięwzięcia Politechniki Warszawskiej, HEC School of Management Paris, London Business School oraz NHH Norwegian School of Economics. Szkoła od lat jest pełnoprawnym członkiem prestiżowej organizacji European Foundation for Management Development, utworzonej przez wiodące europejskie szkoły zarządzania.

Misją Szkoły jest oferowanie liderom biznesu i ekspertom najwyższej klasy praktycznych programów edukacyjnych, tworzonych w oparciu o najlepsze międzynarodowe praktyki, innowacyjne podejście oraz zgodnie z rozwojem technologicznym i zasadą pozytywnego wpływu społecznego.

**\*\*\***

**Kontakt dla mediów:**

**Mariusz Jaroń**

[**m.jaron@comunicativo.pl**](mailto:m.jaron@comunicativo.pl)

**794490680**