***Kontakt dla prasy:***

*Agnieszka Juraszczyk*

*+48 883 357 638*

*E-mail:* [*agnieszka.juraszczyk@capgemini.com*](file:///C:\Users\ajuraszc\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\4TKWL6WX\agnieszka.juraszczyk@capgemini.com)

***Kontakt dla prasy:***

*Aleksandra Witkowska*

*+48 693 407 831*

*E-mail:* [*aleksandra.witkowska@linkleaders.pl*](mailto:aleksandra.witkowska@linkleaders.pl)

**Cztery domeny cybersecurity. Różnorodność ról w branży cyberbezpieczeństwa**

**Szacuje się, że w 2021 roku w Polsce w branży cyberbezpieczeństwa było ok. 17 500 nieobsadzonych stanowisk.[[1]](#footnote-1) Ten niedobór pracowników nie maleje, branża rozwija się w ujęciu wykładniczym, na rodzimym rynku na jednego kandydata przypada ok. 7 nieobsadzonych stanowisk – zarówno wśród ekspertów z dużym doświadczeniem, jak i młodszych specjalistów oraz stażystów, czyli kandydatów z poziomu tzw. *entry level*. Możliwości rozwoju na ścieżce cyberbezpieczeństwa jest wiele, a branża stale rozwija się, odpowiadając na pojawiające się wyzwania – jakie trendy będą widoczne w cybersecurity najbliższych miesiącach? Jakimi obszarami warto się zainteresować? Oto cztery z nich.**

**Bezpiecznie jak w chmurze – Cloud Security**

Chmura napędza coraz więcej dziedzin naszego życia i usług korporacyjnych, z których korzystamy na co dzień, dlatego wszystkie podmioty, które rozwijają rozwiązania chmurowe traktują bezpieczeństwo danych priorytetowo. Bezpieczeństwo chmury to cały pakiet technologii, protokołów i najlepszych praktyk, które chronią środowiska przetwarzania, aplikacje i dane przechowywane w chmurze. Aby środowisko to było bezpieczne, należy pamiętać nie tylko o technologii, ale i zarządzaniu oraz procedurach. Fragmentacja spowodowana wykorzystaniem wielu rozwiązań chmurowych oraz środowisk hybrydowych, jak i złożoności ekosystemów w jakich funkcjonują firmy, prowadzi często do zwiększenia podatności na ataki oraz utrudnia zarządzanie bezpieczeństwem.

* Jesteśmy w okresie transformacji z rozwiązań tradycyjnych do chmury. Klasyczna infrastruktura wzbogaca się o rozwiązania chmurowe, ale tradycyjne rozwiązania wciąż pozostają w użyciu i będą z nami jeszcze co najmniej kilka lat. Eksperci z branży cybersecurity muszą więc posiadać szerokie kompetencje w zakresie analityki i monitoringu. Ich wykorzystanie pozwoli utrzymywać wysoki poziom bezpieczeństwa infrastruktury, a zwłaszcza dostępu do danych współdzielonych i zlokalizowanych w chmurze. Musimy szybko reagować na wszelkie pojawiające się zagrożenia lub wykryte luki – mówi **Rafał Pluta, Head of Cybersecurity w Capgemini Polska.**

Prawdziwa wartość architektury bezpieczeństwa wykorzystującej chmurę opiera się na aktywnej komunikacji pomiędzy szerokim gronem interesariuszy oraz na prostych i przejrzystych regułach. Usługi cybersecurity wykorzystują wiedzę ekspertów oraz najnowsze trendy technologiczne dostępne na rynku w celu ochrony zasobów organizacji. Ponadto w Capgemini stosuje się zasadę: „think as threat actor do”, która pozwala opracowywać procedury bezpieczeństwa. Odpowiednio przyjęta strategia to podstawa budowy bezpiecznej chmury i ten aspekt będzie mocno rozwijał się w najbliższej przyszłości.

**Zarządzanie tożsamością i dostępem**

Kolejny obszar cyberbezpieczeństwa, na który warto zwrócić uwagę to zarządzanie tożsamością i dostępem (ang. IAM, *Identity and Access Management*). Jest to część cybersecurity, która odpowiada za tożsamości cyfrowe i dostęp użytkowników do danych, systemów i zasobów organizacji. Zabezpieczenia IAM obejmują zasady, programy i technologie, które zmniejszają ryzyko dostępu osób niepowołanych do danych firmowych. Identyfikacja, uwierzytelnianie i autoryzacja użytkowników, przy jednoczesnej kontroli dostępów nieupoważnionych – na tym koncentrują się systemy IAM. To jedno z najskuteczniejszych narzędzi zabezpieczających przed zagrożeniami wewnętrznymi, w znaczący sposób wpływające na zmniejszenie liczby incydentów nieautoryzowanego dostępu. Narzędzia i systemy typu IAM są doskonałym rozwiązaniem do zarządzania ryzykiem oraz bezpieczeństwem organizacji.

* Role związane z zarządzaniem tożsamością i dostępem mogą obejmować bardzo wiele obszarów, począwszy od usług katalogowych tożsamości, zapewniania i usuwania dostępu użytkowników, wdrażanie technologii IAM jako takiej, wraz z powiązaną infrastrukturą, czy praca nad bezpieczeństwem cyklu rozwoju aplikacji, audyty, testowanie, identyfikowanie wraz z obsługą wyjątków i wiele innych aspektów. Te role w organizacji mają kluczowe znaczenie pod kątem oceny ryzyka oraz wewnętrznego i zewnętrznego bezpieczeństwa organizacji. To wymaga od kandydatów umiejętności zarówno analitycznych, jak i miękkich – wiele ról IAM wymaga wiedzy technicznej, jednak jest też personel nietechniczny, który zajmuje się również analizą biznesową, zarządzaniem ryzykiem, audytem, ​​zarządzaniem projektami i innymi obszarami. IAM to, być może wbrew pozorom, bardzo szeroka specjalizacja, która daje duże możliwości rozwoju – dodaje **Rafał Pluta.**

**GRC, czyli zarządzanie, ryzyko i zgodność**

GRC (ang. G*overnance, Risk & Compliance*) to z kolei obszar, który określa się jako mierzalny sposób obserwacji zasad i polityk firmowych, przy jednoczesnym przewidywaniu problemów w organizacji i procedur zarządzania tym procesem jako całością. Zmieniająca się dynamika biznesu i nowe technologie wymagają synchronizacji tych trzech czynników – zarządzania, ryzyka i zgodności. Zarządzanie odnosi się do podejmowania decyzji, a ryzyko opisuje czynniki, które mogą narazić organizację na niebezpieczeństwo. Ryzyka można zidentyfikować jako zagrożenia zewnętrzne lub wewnętrzne (drobne lub krytyczne). Zgodność obejmuje z kolei obszar prawa i regulacji.

Istnieje wiele możliwych ról, które można objąć w obszarze GRC – na poziomie podstawowym mogą to być role oparte na praktycznych aspektach zarządzania ryzykiem, takie jak przygotowywania polityk, ocena ryzyka i zgodność z istniejącymi zasadami. Na stanowiskach obejmowanych przez specjalistów z większym doświadczeniem w zakresie cyberbezpieczeństwa, większa będzie także odpowiedzialność związana z zapewnieniem zgodności. Dla przykładu, identyfikując potencjalne zagrożenia, należy znać aktywa organizacji i ich wartość, dlatego wymaga to regularnych rozmów z interesariuszami w całej organizacji oraz wiedzy, jak przechowywane są dane organizacji i jak przepływają między systemami. Podobnie, podczas oceny prawdopodobieństwa i wpływu ryzyka wpływającego na system lub zestaw informacji, należy ściśle współpracować z osobami z zespołu odpowiadającymi za pozostałe aspekty związane z bezpieczeństwem cybernetycznym, w szczególności w zakresie zarządzania lukami w zabezpieczeniach i analizy zagrożeń.

**Dedykowane centra bezpieczeństwa – SOC**

Dedykowane centra operacji związanych z bezpieczeństwem (SOC, ang. *Security Operations Center*) to zewnętrzne jednostki, w których funkcjonują zespoły ds. bezpieczeństwa informacji odpowiedzialne za bieżące monitorowanie i analizę stanu bezpieczeństwa organizacji. Celem zespołów SOC jest wykrywanie, analizowanie i reagowanie na incydenty związane z cyberbezpieczeństwem przy użyciu kombinacji rozwiązań technologicznych i procesów. Centra operacji bezpieczeństwa zazwyczaj zatrudniają analityków i inżynierów ds. bezpieczeństwa, a także menedżerów, którzy nadzorują operacje związane z bezpieczeństwem. Pracownicy SOC ściśle współpracują z zespołami reagowania na incydenty w organizacji, aby zapewnić szybkie rozwiązywanie problemów związanych z bezpieczeństwem po ich wykryciu.

* W Capgemini uruchomiliśmy niedawno taki ośrodek bezpieczeństwa w Katowicach – tu mieści się nasze Cyber Defense Center. Tego rodzaju rozwiązania stają się coraz powszechniejsze na świecie, ponieważ dzięki nim jesteśmy w stanie wielu klientom korzystającym z jednej, dopracowanej przez nas platformy zapewnić ochronę ich indywidualnych systemów. Tym samym klienci korzystający z takiego zewnętrznego centrum uzyskują łatwy i szybki dostęp do najnowszych kompleksowych rozwiązań bezpieczeństwa, mając dodatkowo możliwość z usług SOC w modelu SOCaaS – mówi **Beniamin Poznański, Head of CIS P&C Eastern Europe, w Capgemini Polska.**

Zespoły funkcjonujące w ramach SOC muszą być różnorodne z uwagi na charakter takiego rodzaju jednostek – organizacjom oferuje się najlepsze dostępne systemy zabezpieczeń, ale także potencjał zróżnicowanego grona ekspertów. W takich zespołach funkcjonują analitycy, inżynierowie odpowiedzialni za budowę i utrzymanie systemów oraz managerowie, którzy nadzorują operacje. Karierę w tym zakresie najlepiej rozpocząć na stanowisku analityka, a stąd możliwe jest kilka ścieżek rozwoju.

Według najnowszego raportu Światowego Forum Ekonomicznego (WEF), na świecie brakuje 3 milionów specjalistów ds. cyberbezpieczeństwa, a ten niedobór jest jednym z głównych wyzwań firm technologicznych w 2022 roku. Istnieje niedostateczna podaż specjalistów cybernetycznych — na całym świecie brakuje ekspertów, którzy mogą zapewnić bezpieczny rozwój cyberprzestrzeni, testować i zabezpieczać systemy oraz szkolić ludzi w zakresie higieny cyfrowej. Zapotrzebowanie na specjalistów ds. cyberbezpieczeństwa jest ogromne, a choć większość osób pracuje przez co najmniej rok lub dwa w IT, zanim przejdzie do pracy w zakresie bezpieczeństwa, to dziś podaż jest tak duża, że szansę na wejście w ten świat mają również osoby początkujące. Ścieżek rozwoju w branży bezpieczeństwa cyfrowego jest wiele, a rynek jest bardzo atrakcyjny i wbrew branżowemu powiedzeniu, że „nie ma czegoś takiego jak praca na poziomie podstawowym w cybersecurity”, dostępność tego zawodu jest coraz większa.

**O Capgemini**

Capgemini to światowy lider w dziedzinie doradztwa w zakresie transformacji i zarządzania biznesem poprzez wykorzystanie mocy technologii. Celem Grupy jest dążenie do odpowiedzialnej społecznie, zintegrowanej i zrównoważonej przyszłości, w której potencjał ludzki jest wspierany nowymi technologiami. Capgemini jest odpowiedzialną i wielokulturową organizacją, liczącą ponad 325 000 pracowników zatrudnionych w ponad 50 krajach. Dzięki silnemu 55-letniemu dziedzictwu i szerokiej wiedzy branżowej cieszy się zaufaniem swoich klientów, a także jest zdolna kompleksowo zaspokoić ich potrzeby biznesowe: od strategii i projektowania rozwiązań po działania operacyjne napędzane przez dynamicznie rozwijający się i innowacyjny świat technologii chmury, danych, sztucznej inteligencji, łączności, oprogramowania, inżynierii cyfrowej i platform. W 2021 roku Grupa odnotowała globalne przychody w wysokości 18 miliardów euro.

Get The Future You Want | [www.capgemini.com](http://www.capgemini.com#_blank)

1. HackerU, *Cybersecurity. Raport o rynku pracy w Polsce,* 2021 [↑](#footnote-ref-1)