accenture

POINTS OF CHANGE – CYBERSECURITY

VIDEO TRANSCRIPT

/Intro/
Cyberbezpieczeństwo to temat równie gorący, jak i zaniedbany. Z jednej strony coraz więcej mówi się o zagrożeniach, jakie niesie ze sobą rozwój technologii, a z drugiej najczęściej używanym hasłem na świecie jest po prostu 123456. Na szczęście mamy specjalistów, którzy dbają o nasze bezpieczeństwo. Czy praca w cyberbezpieczeństwie wiąże się wyłącznie z kodowaniem? Czy filmowe sceny, w których zakapturzona postać wpisuje linijkę po linijce kodu odwzorowują rzeczywistość? Czy jest jeszcze miejsce na rynku dla nowych ekspertów? Albo raczej - jak wielu z nich brakuje? W Accenture pracuje kilka tysięcy specjalistów od cyfrowych zabezpieczeń. Jednej z tych osób zadam te i inne pytania.
Nazywam się Krzysztof Kobyłecki a rozmawiać ze mną będzie Olga Budziszewska - Security Strategy Consultant w Accenture.

/wstawka fabularna/
Hania: Hej Pomocnik! Włącz ekspres do kawy.
Pomocnik: Nie ma sprawy. Włączam urządzenie: ekspres do kawy. Hania: Hej Pomocnik. Przeczytaj moje trzy pierwsze zadania na dziś.
Pomocnik: Masz dziś dwanaście zadań do wykonania. Pierwsze trzy to: zapłacić rachunki, kupić prezent na urodziny Maćka, napisać maila do zespołu.
Hania: Mój ulubiony dzień miesiąca - dzień płacenia rachunków. Dobra, co my tu mamy? Bank kropka pe el. Login... yhm. I hasło...
Co? Nieudana próba logowania? Jeszcze raz. Login... Hasło… Serwis czasowo niedostępny? Ehh... Spróbuję później.
Hania: Hej Pomocnik, odczytaj najnowszą wiadomość.
Pomocnik: Odczytuję wiadomość od: Bank. Proszę potwierdzić wykonanie transakcji numer jeden, wpisując poniższy kod...
Hania: Stop! Co?!
Maciek: Mamo, co się stało?
Hania: Porozmawiajmy później, dobrze? Maciek: Ale słyszałem krzyk.
Hania: Maćku, nie teraz! Muszę zadzwonić do banku... Maciek: O nie, spóźniłem się!

/rozmowa z ekspertem/
Krzysztof: Cześć Olga! Olga Budziszewska, czyli Security Strategy Consultant w Accenture w Polsce. Olga, czy możesz nam pokrótce powiedzieć co to znaczy Security Strategy Consultant? Jak wygląda Twój typowy dzień? Czym się zajmujesz w Accenture?

Olga: Cześć Krzysztof, bardzo się cieszę, że biorę udział w takim ciekawym podcaście i że będę miała okazję poopowiadać trochę o swojej pracy. Na co dzień w Accenture zajmuję się można powiedzieć bardzo prostymi sprawami, a mianowicie pomagam Klientom Accenture z wielu branż, z wielu sektorów, a także i z wielu krajów w Europie zachować odpowiedni poziom ich cyberbezpieczeństwa, ich bezpieczeństwa informacji, tak aby ich dane osobowe, wrażliwe dane firmowe po prostu były bezpieczne.

Krzysztof: Czyli dbasz o bezpieczeństwo i dbasz o bezpieczeństwo w tej takiej cyfrowej sferze. Cyberbezpieczeństwo jest dziś tematem naszej rozmowy. A czy możesz nam zarysować troszeczkę szerzej niż zrobiłaś to do tej pory, czym tak naprawdę jest cybezbezpieczeństwo? Kojarzy nam się zawsze, przynajmniej jak ja słyszę cyberbezpieczeństwo od razu odpalają

mi się jakieś filmy w głowie, hakerzy, lata 90-te, Matrix, hakowanie, kod płynący przez ekrany… a czym tak naprawdę jest cyberbezpieczeństwo w takim życiu codziennym, gdzie pracuje się z różnymi Klientami. Co możesz nam powiedzieć o cyberbezpieczeństwie?

Olga: Widzisz, cyberbezpieczeństwo to nie tylko technologia. Cyberbezpieczeństwo to jest technologia, procesy i ludzie. A technologia nie może działać w oderwaniu od biznesu, a ponieważ biznes tworzą ludzie, tworzą procesy, są produkty, są procesy, są usługi, które trzeba chronić i cyberbezpieczeństwo właśnie jest skierowane na to, żeby pomóc biznesowi w sposób bezpieczny, w sposób zaufany świadczyć swoje usługi.

Także cyberbezpieczeństwo to o wiele, wiele więcej niż tylko to co widzimy na filmach. Fajnie, że możemy to w ogóle oglądać, tak? Seriale typu Mr Robot, czy filmy, wiadomo, z udziałem popularnych aktorów i to rzeczywiście jest bardzo ciekawe i jest to element naszej codziennej pracy. Tak samo jak elementem naszej codziennej pracy jest też obserwowanie tego w jaki sposób cyberprzestępcy działają, tak? Czyli na przykład historie typu historia Kevina Mitnicka zawsze będzie dla nas ciekawa i będziemy sobie ją czytać. Natomiast czy my rzeczywiście na co dzień spotykamy się z aż takim, można powiedzieć,budzącym emocje procesem? No pewnie nie, ale tak to chyba jest w każdej branży, tak? Natomiast mamy tak czy inaczej bardzo dużo pracy, no szczególnie ostatnio, tak?

Krzysztof: Czy możesz powiedzieć jaka jest taka definicja cyberbezpieczeństwa? Wspomniałaś o ludziach, procesach i technologii. Czy cyberbezpieczeństwo to jest zadbanie o wszystkie styki pomiędzy tymi trzema rzeczami, czy jest to coś więcej? Jaka jest taka Twoja definicja cyberbezpieczeństwa?

Olga: Rzeczywiście jeżeli chodzi o taka ogólnie przyjętą definicję cyberbezpieczeństwa, to tu pewnie Ci jej nie przytoczę. Natomiast to co tu jest dla nas najważniejsze z punktu widzenia jakby pracy u Klienta, to jest takie holistyczne podejście do cyberbezpieczeństwa. I to jest jakby też temat, który jest w tej chwili najbardziej aktualny i najczęściej podejmowany w rozmowach z naszymi Klientami, żeby ich przekonać do tego, że cyberbezpieczeństwo ich organizacji, ich firmy, to nie jest tylko praca działu IT, czy praca działu IT z działem bezpieczeństwa. To tak naprawdę jest praca całej organizacji. Bo jeżeli większość danych firmy przenosi się w świat wirtualny, w świat online to siłą rzeczy wszystkie te dane muszą być odpowiednio zabezpieczone. A jeżeli już mówimy o takich frameworkach bardzo popularnych ogólnie przyjętych, to musimy te dane ochronić, zabezpieczać, musimy identyfikować zagrożenia jakie są na tych danych. Musimy odpowiednio reagować na incydenty bezpieczeństwa i musimy mieć możliwość, w razie wystąpienia takiego incydentu bezpieczeństwa, musimy mieć możliwość odzyskania tych danych, tych informacji, które no po prostu w jakiś sposób utraciliśmy. Także cyberbezpieczeństwo to jest bardzo holistyczny proces, który obejmuje praktycznie całą organizację, nastawiony na to, aby zadbać o bezpieczeństwo informacji i danych danej organizacji, tak żeby ta organizacja mogła w sposób skuteczny i efektywny świadczyć swoje usługi, nawet w sytuacjach kryzysowych typu atak hakerski, incydent bezpieczeństwa, czy to co nas dzisiaj spotyka, czyli przeniesienie się do świata wirtualnego i niemożność pracy np. w ramach architektury korporacyjnej w biurach.

Krzysztof: Okej. Ty specjalizujesz się w pewnym rodzaju cyberbezpieczeństwa, czyli jesteś związana z zabezpieczaniem rozwiązań chmurowych. Czy możesz coś więcej powiedzieć o tym obszarze?

Olga: Słuchaj, to jest w ogóle fascynujący obszar i ja tutaj prowadzę wiele różnych działań, kampanii zachęcających właśnie ludzi do wejścia w ten świat chmury, ponieważ to jest taki obszar bardzo dynamicznie się rozwijający. Rozwija się przede wszystkim dlatego, że biznes, że organizacje bardzo potrzebują w tej chwili skorzystać z chmur. To co się stało ostatnio w kontekście COVIDu, to, że większość naszego życia się przeniosła do świata online. Tutaj mogę podać taką jedną statystyczną liczbę, szacuje się, że przed COVIDem około 27% pracowników globalnie pracowało w trybie zdalnym, a po tych kilku miesiącach jest już ich ponad 60%. Słuchaj - to jest ogromny wzrost, tak to wszystko

przeniosło się do cloudu i to ma ogromny wpływ na całą strategię bezpieczeństwa organizacji, ponieważ to bezpieczeństwo w chmurze działa na zupełnie innych zasadach niż to tradycyjne bezpieczeństwo, z którym mieliśmy do czynienia do tej pory. Wiesz, tutaj jest kilka takich poważnych wyzwań: przede wszystkim w jaki sposób ustawić sobie poziom odpowiedzialności pomiędzy tym za co my odpowiadamy w ramach naszej firmy, a za co odpowiada dostawca chmury, z którego zdecydowaliśmy się usług skorzystać. To się tak nazywa model współdzielonej odpowiedzialności.

Krzysztof: Tak naprawdę zadaniem cyberbezpieczeństwa jest to, żeby biznes działał, tak? Nie ma dojść do żadnego ataku, który może spowodować to, że coś się stanie z biznesem, który jest Waszym Klientem. Jakie są Twoim zdaniem takie najczęstsze wypadki, które zdarzają się Waszym Klientom, albo przeciw czemu
działacie w Accenture jeśli chodzi o Waszych Klientów?

Olga: To jest tak, że nie tyle rolą bezpieczeństwa jest przeciwdziałanie temu, żeby coś się zdarzyło bo tego nigdy nie będziemy na 100% pewni. Bo właściwie to możemy być na 100% pewni, że na pewno będziemy celem ataku. Teraz czy uda nam się to odeprzeć to jedna sprawa, a druga sprawa to jest co zrobimy i w jaki sposób jesteśmy przygotowani do takiej sytuacji, kiedy nie uda nam się tego odeprzeć, tak? I to jest ogromny obszar, którym też bezpieczeństwo musi się zająć.

Krzysztof: Czyli powiedziałabyś, że są dwie strony? Z jednej strony to jest prewencja i dbanie o to, aby różnego rodzaju ataki nie nastąpiły. Z drugiej strony to jest odbijanie ataków? Czy istnieje taki podział? Jak to widzisz?

Olga: Tak oczywiście istnieje taki podział plus jeszcze inny, tak? Mamy wiesz, tutaj można powiedzieć jakby idąc od samego początku, tak? Czyli najpierw mamy zdolność organizacji do, w ogóle, zidentyfikowania zagrożenia jakie są na rynku i to jest cały ten obszar threat intelligence - to się nazywa, czyli jakby
monitorowania tych zagrożeń, które są na rynku, czy mamy do tego odpowiednie technologie, czy mamy do tego odpowiedni zespół, czy jesteśmy w stanie w ogóle to monitorować, tak? Czyli identyfikować jakie mamy zagrożenia. Potem czy my jesteśmy w stanie wykryć, czy te zagrożenia dotyczą naszej organizacji, ponieważ monitorujemy całość, a część dotyczy naszej organizacji. Jeżeli to dotyczy naszej organizacji, to musimy mieć możliwość w jakiś sposób odpowiedzieć na to zagrożenie, czyli mieć odpowiednie, jakby mechanizmy obronne, na ten atak. Niech to będzie nawet ransomware – nas dosięgnie i zaszyfruje wszystkie dane na dyskach, czy my jesteśmy w stanie odpowiednio zareagować, odpowiedzieć i się z tego wykaraskać krótko mówiąc. Czy mamy np. kopie zapasowe utrzymywane w innej lokalizacji, z których
jesteśmy w stanie podnieść nasze systemy. Tak, że ta ścieżka, którą zajmuje się cyberbezpieczeństwo jest od samego początku do samego końca, przy czym w ramach samego cyberbezpieczeństwa, w ramach
zespołów, jeżeli mówimy już o takich super zaawansowanych zespołach też mamy różne kompetencje, różne zakresy. Strategia blue team - red team, czyli mamy dwa teamy w ramach naszych zespołów. Jeden zespół cały czas atakuje nasze systemy, nasze środowisko, drugi zespół cały czas ma za zadanie je bronić. Najlepiej jak te zespoły potem się mieszają, czyli członkowie tych zespołów potem się zmieniają tak, żeby cały czas odnajdywać nowe możliwości ataku i nowe możliwości obrony. Ale to wiesz, to są takie bardzo zaawansowane rzeczy na tej skali… powiedzmy pięciostopniowej skali dojrzałości, to jest duża dojrzałość. Mi się wydaje, że my tutaj, w Polsce szczególnie, jeszcze jesteśmy na dużo niższych poziomach, borykamy się z jeszcze mniej skomplikowanymi wyzwaniami.

Krzysztof: Wy jako Accenture jesteście organizacją, która w sumie ma powodować zmiany. Let there be change jest jednym z takich Waszych brand purposes, więc mam nadzieję, że będziecie wznosić organizacje do tego piątego poziomu, jeśli chodzi o cybersecurity, czyli cyberbezpieczeństwo.

Olga: Każdy ten kolejny poziom wymaga budżetu i powiem Ci, że jakbym miała mówić takie największe
bolączki na dzień dzisiejszy, z którymi branża się boryka to też jest coś takiego, że wewnątrz

firm, wewnątrz organizacji bezpieczeństwo jeszcze nie jest traktowane w ten sposób, że ma bezpośrednie przełożenie na biznes z tego powodu, że zawsze udawało się jakoś z tych incydentów bezpieczeństwa wyjść cało. W momencie, kiedy coraz więcej naszego biznesu jest świadczona tylko online, to po prostu konsekwencje tych ataków będą dla biznesów coraz gorsze, coraz bardziej dotkliwe.

Krzysztof: Budżety na cyberbezpieczeństwo to jest jedna sprawa, ale to jest też bezpośrednio powiązane z tym jak wygląda sytuacja na rynku. Niektóre raporty, które są dostępne w Waszej organizacji a propos cyberbezpieczeństwa mówią o tym, że w samym roku 2000 o 60% skoczyły kwoty, które hakerzy chcą wyciągnąć od organizacji. A na naszym polskim rynku mamy parę takich ataków, które pokazują, że te kwoty z roku na rok, z miesiąca na miesiąc są coraz większe. Strategie jeśli chodzi o negocjacje zazwyczaj mówią o tym, aby jednak nie decydować się na zapłatę hakerom, czyli z jednej strony mamy to, że podczas danego ataku możemy być narażeni na jakąś sumę pieniężną, z drugiej strony mamy sumę pieniężną, którą musimy my w naszej organizacji wydzielić na to żeby nie dopuścić do tych ataków.

Olga: To jest dokładnie tak samo jak z ubezpieczeniami na życie, od choroby, ubezpieczeniami od poważnych chorób. No trudno jest przekonać kogoś, kto jest w bardzo dobrej kondycji fizycznej, żeby teraz

przeznaczał, nie wiem, 10% swojego dochodu na zabezpieczenie się w sytuacji, kiedy zachoruje. Opowiem taką historię, która była bardzo pouczająca. W 2017 roku kiedy globalnie musieliśmy się zmierzyć z konsekwencjami ataku ransomware, to były słynne ataki WannaCry, Petua, które oczywiście tak samo dosięgnęły Polski. To był taki atak, który wykorzystał podatności w starych systemach Windows. To były systemy już nie wspierane przez Microsoft, po prostu wsparcie dla tych systemów się skończyło. Wydaje mi się, że to był taki krok milowy dla bezpieczeństwa, dla działów bezpieczeństwa, także w Polsce. Bo te ataki spowodowały ogromne straty finansowe i wiesz jedna z firm, którą my obsługiwaliśmy akurat w tamtym czasie, to była firma, która dystrybuowała jakieś części do maszyn, czy jakieś takie motoryzacyjne. I oni zostali właściwie pozbawieni funkcjonowania w sposób całkowity. Czyli 90% systemów tej firmy padło, zostało zaszyfrowanych, oni nie mieli dostępu ani możliwości kontaktowania się ze swoimi klientami, klienci nie mieli możliwości kontaktować się z firmą, składać zamówień, a dodatkowym ryzykiem i zagrożeniem było to, że oni musieli złożyć sprawozdanie giełdowe w ciągu 4 dni. Brak takiego sprawozdania jest obciążony ogromnymi karami finansowymi. I wiesz, że tutaj wiele zespołów, wiele firm consultingowych, a także oczywiście ich wewnętrzne zespoły pracowały po 24 h na dobę po to, aby podnieść te systemy, po to, żeby móc wznowić swoje środowisko pracy. Wiesz, wszystko przez to, że nie mieli porządnie zrobionego planu disaster recovery, czyli nie mieli po prostu planu odzyskiwania kopii zapasowych.

Krzysztof: Czy powiedziałabyś, że ataki w sferze cyberbezpieczeństwa są rzeczą tak powszechną i naturalną, że w tym momencie każda organizacja się może tego spodziewać i to jest rzecz, której na pewno trzeba działać przeciwko?

Olga: Tak. Jest takie powiedzonko, że firmy dzielą się na te, które zostały zaatakowane w cyberprzestrzeni i na te, które jeszcze tego nie wiedzą. Takie mamy powiedzonko w branży, bo rzeczywiście ten czas wykrycia, że doszło do ataku cybernetycznego w tej chwili w zależności od tego, które statystyki przytoczymy - ale to jest kilka miesięcy. Kilka miesięcy przestępcy są w systemach organizacji zanim zostaną wykryci. Średnio. To jest ogromny czas. W takim czasie jesteś w stanie przejąć kontrolę absolutnie nad całym systemem. Nowy popularny rodzaj ataku ransom-as-a-service. I nawet nie tyle, że chcą żeby zapłacić jednorazowo, nie wiem 300 dolarów, tak jak było w WannaCry, Petya, tak? Tylko oni chcą miesięcznie, tak jak haracz To jest po prostu jak mafia Miesięcznie chcą pobierać opłatę, ponieważ ty nie jesteś w stanie dojść do tego, w którym momencie oni Cię zaatakowali. Oni są tak długo w twoim systemie, że nie

jesteś w stanie znaleźć miejsca, od którego powinieneś się zrekonstruować jakby. Czyli - które kopie zapasowe powinieneś wziąć. Bo jakby czas odzyskiwania też masz ustalony, że nie wiesz czy masz wziąć sprzed 3 miesięcy, sprzed pół roku, a może oni już są dwa lata i dane są już zmodyfikowane. Bo wiesz w tym bezpieczeństwie przede wszystkim chodzi o to, żeby zachować tę triadę CIA, czyli poufność, integralność, dostępność. To jakbym miała powiedzieć jakąś jedną podstawową zasadę, jaką mam w cyberbezpieczeństwie, no to przede wszystkim ta triada jest najważniejsza.

/wstawka fabularna/
Maciek: Okej, Tomek mówił, że ten gość nagrywa dobre poradniki. “Ludzie nie wiedzą TEGO o inteligentnych urządzeniach”. No to sprawdźmy.
Ekspert na video: Cześć!
Mało kto wie, że nawet haker-amator jest w stanie bez problemu dostać się do sieci, która jest słabo chroniona. A większość ludzi jeszcze ułatwia to, kupując inteligentne urządzenia i nie dbając o ich zabezpieczenia. Wystarczy, że haker wie, które Wi- Fi jest wasze i, używając swojego punktu dostępowego, będzie się w stanie połączyć na przykład z waszym ekspresem do kawy. Te urządzenia są niby takie inteligentne... ale nie do końca. Często mają ustawione domyślne hasła, które hakerzy wyszukują bez trudu. Te hasła należy zmienić przy pierwszej okazji!
Jak haker zaloguje się do ekspresu, to z kolei znajdzie w nim hasło do waszego Wi-Fi, a potem mogą się dziać różne cuda. Na przykład może zaserwować wam podrobioną wersję strony logowania do banku i wykraść wasze dane dostępowe. Nie muszę chyba mówić z czym to się wiąże.
Albo ukradnie wam hasła, o zgrozo!, do mediów społecznościowych.

To się może wydawać zabawne, bo co może wtedy zrobić? Zapostować na waszej tablicy jakieś kompromitujące zdjęcie? No może. Ale po co, skoro może też, podszywając się pod was, napisać do waszych znajomych z prośbą o przelanie pieniędzy na jego konto?
Pamiętajcie, żeby dbać o bezpieczeństwo swojej sieci. A tymczasem dzięki, że oglądaliście mój poradnik. Do zobaczenia w kolejnym odcinku!
Hania: Stop! Co?!
Maciek: Mamo, co się stało?
Hania: Porozmawiajmy później, dobrze? Maciek: Ale słyszałem krzyk.
Hania: Maćku, nie teraz! Muszę zadzwonić do banku... Maciek: O nie, spóźniłem się!
Hania: Co? Znowu coś zmajstrowałeś? Ktoś mi się włamał na konto, muszę do nich szybko zadzwonić.
Maciek: Właśnie się dowiedziałem, że to może być wina ekspresu... Hania: Chyba żartujesz? Zajmiemy się tym, jak załatwię sprawę z bankiem. Maciek: To ja zmienię hasło do ekspresu i naszego Wi-Fi.

/rozmowa z ekspertem/
Krzysztof: Czy możesz powiedzieć o tym jak wygląda taka ścieżka rozwoju, jeśli chodzi o cyberbezpieczeństwo? To znaczy to, że ty pracujesz w cyberbezpieczeństwie, nie wiem jaki masz background. Czy możesz powiedzieć o tym w jaki sposób mogę rozpocząć swoją przygodę z cyberbezpieczeństwem?

Olga: Wiesz co, to jest w ogóle najpiękniejsza sprawa tej całej branży dlatego, że próg wejścia jest bardzo różny. Może być bardzo wysoki, może być też niski i początki mogą być bardzo różne. Oczywiście, że studia informatyczne mogą pomóc, ale nie są konieczne. Wiesz, ja znam mnóstwo ludzi, którzy się świetnie w tym zawodzie odnaleźli, w tej branży odnaleźli i są super specjalistami, w ogóle nie mając do czynienia ani z cyberprzestępczością, ani z IT, ani z żadnymi w ogóle pokrewnymi dziedzinami, a dzisiaj są na przykład rozchwytywanymi pentesterami. Ja sama jestem przypadkiem osoby, która się w ten sposób stransformowała. Może tak nie do końca, ale ja skończyłam kryminologię i zawsze przestępczość mnie interesowała i tak naprawdę zostało też tak trochę do tej pory. Dlatego bardzo mnie też interesują te tematy motywacji, tego w jaki sposób podejść do cyberprzestępczości, jak z nią walczyć, jak zapobiegać. Natomiast krótko po studiach od razu zrobiłam kolejne studia podyplomowe już stricte z bezpieczeństwa informacji. No i to mi dało jakby wejście do pracy w firmie technologicznej, a jak już weszłam do firmy technologicznej, to po prostu szkoliłam się i

zdawałam coraz to kolejne certyfikaty, zresztą nadal to robię. I te certyfikaty wydają mi się tutaj takim ciekawym tematem, bo mamy certyfikaty zarówno po stronie organizacyjno-procesowo-zarządzania, jak i po stronie technologicznej. Wydaje mi się, że tutaj każdy kto jest zainteresowany rozwojem swojej ścieżki kariery w cyberbezpieczeństwie jest w stanie znaleźć dużo ciekawych punktów wejścia do branży, tak? Czy chce się zająć na przykład zarządzaniem bezpieczeństwem i wtedy mamy certyfikaty, które daje na przykład ISACA. Czy chce się zająć bardziej wsparciem bezpieczeństwa, ale po stronie IT, wtedy po prostu certyfikuje się z konkretnych technologii albo z takiej organizacji, która nazywa się (ISC)². Czy jest zainteresowany bezpieczeństwem chmury, wtedy certyfikację z Cloud Securitu Allienace, czyli takiej organizacji, która się specjalizuje właśnie w chmurze. Ja poszłam tą drogą Cały czas się te certyfikacje rozwijają, pojawiają się nowe szkolenia. No zdecydowanie muszę Ci powiedzieć, że to jest taka praca, w której uczysz się całe życie. I uczysz się… no każdy miesiąc przynosi coś nowego, tak? To jest tak trochę jak z lekarzami. No wyobraź sobie, że ja bym miała się zatrzymać na tym świecie, który znałam 10 lat temu, który my żeśmy wszyscy znali 10 lat temu, jak bardzo był on inny w kontekście technologii. Jak zupełnie inne były wyzwania i sposoby obrony, tak?

Krzysztof: Jak szybko w takim razie zmienia się ta branża cyberbezpieczeństwa? Zarówno po stronie osób, które bronią, jak i po stronie osób, które atakują. Czy wy musicie podążać za trendami w cyklach miesięcznych, kwartalnych, rocznych? Jak często pojawiają się kompletnie nowe sposoby ataków?

Olga: branża zmienia się dokładnie tak samo, jak zmienia się cyfryzacja naszej gospodarki. Ponieważ ja tak zawsze mówię, że cyberbezpieczeństwo jest w jakiś tam aspekcie młodszą siostrą transformacji cyfrowej. ponieważ ona idzie za transformacją cyfrową. Im więcej mamy rzeczy w świecie wirtualnym, tym więcej rzeczy musimy bronić. Czy to się zmienia w cyklach miesięcznych? Nie no, myślę, że tak nie możemy powiedzieć. Natomiast na pewno możemy powiedzieć, że ta sytuacja, której dziś doświadczamy, to jest wywrócenie wszystkiego do góry nogami. Naprawdę myślę, że nie jesteśmy jeszcze nawet gotowi, żeby oceniać. Pomimo, że jest w tej chwili bardzo dużo raportów, analiz, wszystkie firmy zajmujące się cyberbezpieczeństwem, od programów antywirusowych, czy innych firm, które, nie wiem, świadczą usługi bardziej holistyczne - wszyscy piszą o tym, w jaki sposób zmienia się ten świat cyberbezpieczeństwa. Ale ja mam takie poczucie, że my jeszcze tego nie wiemy, tak? Jesteśmy w trakcie tej całej sytuacji, jeszcze nie wiemy, gdzie będziemy za pół roku.

Krzysztof: Na pewno jednym z większych wyzwań jest praca zdalna i to, że wszyscy pracownicy, większość pracowników firm pracuje z domu, a nie pracuje z bezpiecznej infrastruktury firmy, która była budowana od lat. Czy możesz powiedzieć coś więcej o tym w jaki sposób Accenture poradziło sobie z przejściem na pracę zdalną i zadbaniem o cyberbezpieczeństwo? Jesteście jedną z organizacji na świecie, która sprawnie sobie z tym poradziła. Czy możesz coś więcej o tym powiedzieć?

Olga: Słuchaj, no Accenture sobie poradziło z tym sprawnie, bo Accenture pracuje zdalnie już od długiego czasu, a przynajmniej od czasu w którym ja jestem w Accenture. Tak, że ja nigdy inaczej nie pracowałam. Ja pracowałam wcześniej w zespole globalnym, dołączyłam do zespoły security całkiem niedawno - do Polskiego zespołu security dołączyłam całkiem niedawno. Tak, że ja zawsze pracowałam zdalnie będąc tutaj i jakby dla mnie to zupełnie, no poza tym, że nie mogę pójść po prostu do biura, tak, żeby się z kimś spotkać, to nie ma żadnej różnicy. I wiesz Accenture było na to już od dawna przygotowane. Natomiast ja pracuję z klientami, którzy się z tym borykają i tutaj problemów jest bardzo dużo. Począwszy od zabezpieczenia technologii i urządzeń na jakich pracownicy pracują. No bo tutaj wyjmujesz człowieka z tej architektury korporacyjnej, tak? Zbudowałeś sobie jakiś system bezpieczeństwa w ramach jakiejś architektury korporacyjnej. Wyjmujesz, nie wiem, 60% pracowników, rozpraszasz ich i dajesz im narzędzie cloudowe do tego, żeby się porozumiewali. W tym narzędziu cloudowym wrzucasz też wszystkie bardzo poufne i wrażliwe

dane. Ludzie się łączą ze swojego własnego Internetu, często nie potrafiąc go odpowiednio skonfigurować. No, tu jest jakby nauka u podstaw użytkowników. Często komputery są dzielone z innymi członkami rodziny – wiadomo, bo taka jest potrzeba. Jakby tych problemów pojawiło się wiele. Takich, o których nie mieliśmy pojęcia. Czyli to dbanie o bezpieczeństwo tego użytkownika
końcowego w kontekście też urządzenia, zabezpieczenie jego tożsamości, to jest teraz taka fajna dziedzina, która bardzo się rozwija i to jest też super punkt wejścia w ogóle do zawodu. To jest to bezpieczeństwo tożsamości cyfrowej - digital identity. W jaki sposób mamy zabezpieczyć już nie zamek w środku, tak? Tylko tych wszystkich ludzi, którzy są poza zamkiem, czyli ta koncepcja zero trust security, czyli nie ufaj nikomu.

Krzysztof: Czyli jednak rozchodzenie na te wszystkie końcówki ludzkie i wychodzenie poza ten zamek. Czy
możesz powiedzieć jakie są ścieżki kariery w Accenture, jeśli chodzi o cyberbezpieczeństwo?

Olga: W zespole cybersecurity w Accenture Polska mamy 5 takich ścieżek rozwoju. Pierwsza ścieżka to jest ta, którą ja reprezentuję. To jest strategy and risk. Są też wszystkie tematy compliancowe, których dzisiaj żeśmy tutaj nie podjęli, ale one też są bardzo ważne. Czyli te wszystkie sprawy związane z wymaganiami prawno-regulacyjnymi, RODO, komunikaty KNFu, dyrektywy NIS, tak? To są wszystkie te rzeczy prawno- regulacyjne, które stawiają ramy tego cyberbezpieczeństwa, szczególnie dla organizacji, które działają w tych regulowanych sektorach. Mamy oczywiście tę całą, ogromną odnogę cyber defense, czyli po prostu tej obrony przed cyberatakami, pomaganie klientom w zorganizowaniu ich security operation center, czyli tego monitorowania bezpieczeństwa i odpowiadania na ataki. Jest zespół bardzo prężnie się rozwijający - digital identity - to o czym mówiłam - czyli obrona tożsamości. Tutaj wychodzi na przeciw zarówno technologia, jak i procesy. Bo wiesz - żeby to wszystko ogarnąć, no to trzeba odpowiednio zarządzać uprawnieniami i tożsamościami. Mamy dział, który się nazywa OT Security, czyli ten cały dział bezpieczeństwa automatyki przemysłowej, który też na szczęście staje się coraz bardziej ważny i coraz więcej projektów w tym zakresie również się pojawia, choć jest to rzeczywiście temat wschodzący i jeszcze trudny do przebicia się w Polsce.

Ale coraz więcej projektów, w tym temacie się pojawia, coraz więcej ludzi my w tym obszarze zatrudniamy. No i na koniec oczywiście perełka - cloud security, to jest mój obszar, ja jestem na styku strategy and risk, rozwijając własne projekty w obszarze cloud security.

Krzysztof: Jakiego rodzaju zespoły działają nad tego typu projektami? Jak wyglądają te projekty? Jak
wygląda ich wielkość? Co tak naprawdę się dzieje? Czy to jest dobra szansa na rozwój i na naukę?

Olga: Ooo, to jest świetna szansa na rozwój i na naukę - to mogę powiedzieć, że tyle ile się nauczyłam tutaj przez te trochę ponad dwa lata pracując w Accenture, to nie byłabym w stanie sama absolutnie jakoś tego przejść. To nie ma nawet mowy o tym. Bo ja tam, abstrahując od ścieżek szkoleniowych, bo Accenture daje też dużo możliwości takich typowo szkoleniowych, czyli budżet szkoleniowy, możliwość uczestnictwa w szkoleniach wewnętrznych jak i zewnętrznych. Czyli te wszystkie certyfikaty, o których mówiłam, to jest jakby jedna ścieżka i Accenture bardzo wspiera pracowników w takich działaniach edukacyjnych. A druga sprawa to jest udział w samych projektach. Widzisz - Accenture jest taką fajną firmą, która patrzy na te projekty z bezpieczeństwa bardzo holistycznie. Ponieważ jak ja, powiedzmy, pracuję w zespole strategy and risk, to ja budując strategię bezpieczeństwa buduję ją już w taki sposób, żeby moi koledzy z następnych
zespołów, które mają już wdrażać te rzeczy, które my żeśmy wymyślili, żeby oni byli w stanie w ogóle to zrealizować. A wiesz, to nie jest taka praktyka powszechna na rynku, ponieważ jeżeli mamy firmy, które robią tylko strategie, łatwo jest zrobić strategię, która jest piękna i do wszystkich pasuje. A zrobić strategię, którą możemy finalnie wdrożyć to już jest - wiesz - to już jest większe wyzwanie.

Krzysztof: No tak, jest zawsze to rozszczepienie między strategią, taktyką, a wdrożeniem.

Olga: Tak. A skoro my, jako Accenture, jesteśmy odpowiedzialni za proces end to end, czyli to ja się muszę jednak wysilić trochę na początku, żeby to miało ręce i nogi, żeby moi koledzy, koleżanki, mogli to potem zrealizować co ja wymyślę. Wiesz, bo ja wiele razy byłam na takich projektach, gdzie czytałam strategie… takie, no wiesz, idealne, które ktoś pisze może niekoniecznie z myślą, że one kiedyś mają zostać wdrożone.

Krzysztof: Wspomniałaś o tym, że w swojej karierze przez ostatnie parę lat nauczyłaś się niesamowicie dużo
rzeczy. Czy możesz podać przykład jakiejś jednej - takiej fajnej rzeczy, której się nauczyłaś jeśli chodzi o
cyberbezpieczeństwo?

Olga: Nauczyłam się czytać skany podatności na przykład. (śmiech) Ja nie wiem czy to jest ciekawe dla kogokolwiek, ale tak. Wiesz co, no ja jestem taka ciekawska i rzeczywiście jak jest jakieś wyzwanie i musimy znaleźć jakiś taki rozsądny sposób na to, żeby jemu podołać, to staram się zgłębić temat na różne sposoby. Poza tym jest jeszcze jedna ogromna rzecz, którą tutaj chciałam koniecznie dzisiaj powiedzieć. To jest to, że jak się pracuje w firmie, która jest tak duża i która ma cały set kompetencji na pokładzie, to to bardzo ułatwia taki rozwój. Bo wiesz, jak ja mam jakiś problem, tak jak z tym na przykład czytaniem skanów podatności, to ja się umawiam na spotkanie z kolegą, koleżanką, która się zajmuje tylko tym i ona po prostu przez 3 godziny mi tłumaczy wszystkie najważniejsze rzeczy, na które ja zapewne musiałabym poświęcić z tydzień żeby się dowiedzieć tegol, co mi ta osoba wytłumaczy. Czyli ten set kompetencji, który my mamy na pokładzie takich specjalistycznych, głębokich - jest ogromną zaletą pracy właśnie w takich większych zespołach cyberbezpieczeństwa.

Krzysztof: Chciałbym z tobą teraz porozmawiać o przyszłości, tak? Jakie Twoim zdaniem są najważniejsze wyzwania, które czekają w cyberbezpieczeństwie w przyszłości? Co się będzie działo? Co roku wypuszczacie bardzo ciekawe raporty, które pokazują trendy w cyberbezpieczeństwie. A co Twoim zdaniem czyha na nas w przyszłym roku?

Olga: Ja nie sądzę, że to się zmieni pod względem jakościowym. Że to się zmieni jakoś zasadniczo od tego, co realizowane było, tego co obserwowaliśmy do tej pory. Wydaje mi się, że to, co na pewno możemy obserwować to skalę. Że ta skala będzie większa, no bo jakby to jest logiczne. Mamy więcej procesów,
więcej danych w cyberprzestrzeni więc skala tych ataków będzie większa. Czy będziemy więcej inwestować
w cyberbezpieczeństwo? Mam wątpliwości, chociaż logicznie by można było sądzić, że… biorąc pod uwagę

wszystkie te badania, o których wspominasz, że wszyscy jednym głosem krzyczą słuchajcie będzie coraz gorzej i jesteście coraz bardziej narażeni, cyberprzestepcy wykorzystują coraz to nowe techniki i technologie, sposoby i wektory ataku. To wydaje mi się, że jednak działy bezpieczeństwa będą średnio
skłonne do tego, żeby inwestować w nowoczesne rozwiązania, z tego względu, że jesteśmy teraz w takim ogólnie finansowym dołku i firmy raczej ograniczają swoje inwestycje, niż je jeszcze powiększają. Jeżeli chodzi o - nie wiem - rodzaje zagrożeń, to tak jak powiedziałam - no ja bym się nie spodziewała tutaj zasadniczych zmian, bo one po prostu nie są konieczne, bo to co się dzieje do tej pory, te mechanizmy, które są do tej pory wykorzystywane, one po prostu działają super i dalej będziemy widzieli mnóstwo kampanii phishingowych, dalej będziemy obserwowali kampanie ransomwarowe i dalej będziemy
edukować naszych klientów, żeby w ogóle budowali plan disaster recovery. Żeby odpowiednio robili kopie zapasowe i dbali o te backupy i żeby wiedzieli jak je mają odzyskiwać. Na pewno dużą pomocą jest automatyzacja, szczególnie w kontekście braku specjalistów na rynku. Bo ten gap kompetencyjny w zakresie, w branży cyberbezpieczeństwa jest bardzo duży. Na pewno będziemy chcieli jakby zwiększać tę armię „cyberbezpieczników” - także to jest dobry czas na to aby wejść do branży.

Krzysztof: Czy możesz w takim razie jeszcze powiedzieć coś o takich umiejętnościach, które powinni
posiadać specjaliści w cyberbezpieczeństwie? Wspomniałaś o tym co nas czeka, jest to duży problem skali, jest to problem budżetów, jest

to problem różnych wyzwań, tak? Natomiast phishing, ransomware, backupy - będzie z nami przez wieki. W takim razie na jakiego rodzaju umiejętności należy zwrócić uwagę, jeżeli chce się zostać specjalistą od cyberbezpieczeństwa?

Olga: No to wiesz, ja mam tutaj dwie perspektywy. Pierwszą perspektywą dla mnie jest to, kogo ja szukam do swojego zespołu. A drugą perspektywą jest to, w jaki sposób ja się chce rozwijać. To mam takie dwie perspektywy. I jeżeli chodzi o perspektywę pierwszą, to kogo my szukamy teraz do zespołu - szukamy ludzi, którzy mają kompetencje i jakiekolwiek umiejętności w tej chwili w zakresie cloudu. Bardzo fajna jest teraz też możliwość rozwoju w obszarze digital identity, o czym już wspominałam. I tutaj mamy takich kilku dostawców, na przykład jak mamy One Identity, CyberArk, Saviynt To są tacy - można powiedzieć - dostawcy z top raportów Gartnera, ten Magic Quadrant - są najbardziej popularni i najszybciej rozwijający się dostawcy - a więc jakby umiejętności i znajomość tych technologii zdecydowanie pomoże w znalezieniu ciekawej pracy, czy możliwości rozwoju właśnie w obszarze digital identity, który będzie się rozwijał bardzo intensywnie przez następne lata. Tutaj nie mam co do tego żadnych wątpliwości.

Krzysztof: Mówi się, że w IT jest stosunkowo mało kobiet. W zeszłym roku znalazłaś się w gronie najbardziej wpływowych kobiet w cyberbezpieczeństwie w Polsce według Fundacji Perspektywy. Chciałem Ci pogratulować. Czy przyniosło Ci to jakieś korzyści?

Olga: Bardzo Ci dziękuję. Było mi bardzo miło, że zostałam w ten sposób wyróżniona - to na początek. Tam chodziło przede wszystkim o to, żeby pokazać takie modelowe role do branży. I ja się znalazłam w gronie 20 dziewczyn, które właśnie odnalazły swoją drogę w cyberbezpieczeństwie w różnych obszarach. Tam każda z nas prezentowała jakiś inny obszar cyberbezpieczeństwa. Była dziewczyna od zbierania cyfrowych dowodów, była pentesterka, była szefowa działu bezpieczeństwa itd. Itd. No i ja akurat w kontekście cloud security, bo rzeczywiście może w kontekście Cloud security nie ma nas jeszcze tak dużo, no z racji tego, że może to jest nowa dziedzina. Ja z chęcią zawsze biorę udział w różnego rodzaju akcjach, jakby promujących udział kobiet w cyberbezpieczeństwie, ale nie ze względów jakichś genderowych czy jakichś, tylko ze względów bardzo pragmatycznych. Po pierwsze bardzo brakuje ludzi do cyberbezpieczeństwa. Bardzo i niezależnie od tego, czy mówimy o kobietach czy o mężczyznach, więc to jest dla mnie pierwszy podstawowy temat. Drugi temat to jest biznesowy. Z mojego doświadczenia, a także z wielu badań wynika, że zespoły różnorodne są dużo bardziej efektywne, skuteczne i dużo bardziej kreatywne i praca w zespołach zróżnicowanych pod względem i kompetencji i płci - tu muszę powiedzieć, tak? No bo tak to niestety jest, no wpływa moim zdaniem na jakość samego projektu. Zdecydowanie tu muszę powiedzieć, bo nie mam co do tego żadnych wątpliwości - we wszystkich projektach, w jakich ja pracuję, kobiety są w mniejszości. Często jestem sama jedna. Jak na przykład projekt, który teraz też realizuję - też jestem sama jedna i wydaje mi się, że moja wartość jest nie tylko taka, że po prostu robię swoją robotę na co dzień najlepiej jak potrafię, to jeszcze do tego wszystkiego wnoszę pewnego rodzaju punkt widzenia na pewne sprawy, tak

chociażby jak na ryzyka związane z danym projektem. Bo jednak troszeczkę inaczej panowie, a inaczej panie to ryzyko nawet na co dzień analizują. Więc tu są te dodatkowe pytania, dodatkowe punkty widzenia wątpliwości i to wpływa bardzo korzystnie na przebieg projektu. No a trzecia sprawa to wiadomo, to jest ta sprawa taka wizerunkowa, tak? To, że tak mało kobiet w cyberbezpieczeństwie jest, bo wszystkim się, że to jest branża bardzo hermetyczna, zamknięta, że to jest jakaś wiedza tajemna, zarezerwowana dla jakichś wyjątkowych specjalistów. Ja bym chciała to bardzo odczarować, bo to jest z wielką krzywdą dla nas wszystkich w tym momencie. Bo ta cyfryzacja weszła we wszystkie możliwe obszary naszego życia i potrzebujemy ludzi, którzy będą czuwać i pilnować naszego bezpieczeństwa w tym obszarze.

Krzysztof: Olga, dziękuję Ci bardzo za rozmowę o cyberbezpieczeństwie, była z nami Olga Budziszewska.

Jeżeli chcecie dowiedzieć się więcej to zapraszam na kolejne odcinki podcastu.

/outro/
Czy jest ktoś, kto nigdy nie zaniedbał żadnego aspektu swojego bezpieczeństwa cyfrowego? Szczególnie w pandemii cyberprzestępcy przyspieszyli. Na szczęście możemy się bronić - często zmieniać hasła, pamiętać, że powinny być złożone, nie klikać w nieznane linki w mailach. Ważne jest także żeby budować świadomość wśród osób mniej obeznanych z tematem. W kwestii pracy w cyberbezpieczeństwie ciekawe jest to, że nie jest to branża tylko i wyłącznie dla programistów. Specjalistka na przykład taka jak Olga, również znajdzie w niej swoje miejsce. Może i ty spróbujesz?
Dziękuję za wysłuchanie tego odcinka i zapraszam do kolejnych. Subskrybuj kanał Points of change w twojej ulubionej aplikacji podcastowej, aby ich nie przegapić. Do usłyszenia przy okazji następnego tematu.
Cześć!