Wszystko, czego wolisz nie wiedzieć o cyberbezpieczeństwie…

Słowo „cyber" jest skrótem od słowa „cybernetics" utworzonego przez profesora Norberta Wienera od starogreckiego słowa κυβερνητικός (kubernētikós), co można przetłumaczyć jako „dobry za sterem". Cybernetykę należy zatem rozumieć jako naukę o teorii komunikacji i sterowania, która zajmuje się przede wszystkim badaniem złożonych systemów, w tym składających się z maszyn i ludzi.

Patrząc na cyberbezpieczeństwo, nie powinniśmy się zajmować wyłącznie technologią, lecz całym uniwersum, w którym ta technologia jest wykorzystywana, czyli całym złożonym systemem wraz z wbudowanymi w niego mechanizmami sterowania (sprzężeniami zwrotnymi).

> *Kluczowa zatem jest funkcja celu, a nie tylko narzędzia, które są wykorzystywane do jego osiągnięcia.*

Obecnie w coraz większym stopniu jesteśmy uzależnieni od technologii. Im młodsze pokolenie, tym bardziej opiera się na informacjach wyszukiwanych w Internecie, często przyjmując je bezkrytycznie. Podobnie, jak znalezione „gotowe" rozwiązania, które są łatwe do wykorzystania metodą „kopiuj-wklej". Automatyka sterująca samochodami czy płatności bezgotówkowe na dobre zagościły w naszym życiu, przykłady można mnożyć. Jak wszystko działa, to często zapominamy właśnie o „sprzężeniu zwrotnym", o sensie sterowania, o wykryciu niekorzystnych zmian i właściwym reagowaniu korygującym ten stan. Wydaje nam się, że wykorzystujemy technologię dla zaspokojenia własnych potrzeb (zawodowych czy prywatnych), tymczasem coraz częściej to ona nami steruje.

> *Chcemy lub nie, wszyscy należymy jednocześnie do obu obozów: „biznesu" i „bezpieczników".*

Cyberbezpieczeństwa nie da się oddzielić od biznesu, tak jak nie da się oddzielić od działalności podstawowej wymagania utrzymania kosztów na racjonalnym poziomie (a przecież nie wszyscy pracujemy w finansach). Powinniśmy działać wspólnie i im szybciej to zrozumiemy, tym będziemy silniejsi. Powinniśmy się uzupełniać i wspierać, a nie ze sobą walczyć. Wzajemne skłócenie jest celem naszych wrogów, bo wtedy łatwiej nas pokonać.

Paweł Henig

absolwent Wydziału Elektroniki Politechniki Warszawskiej. Od połowy lat 90. budował dla centralnej administracji rządowej centra przetwarzania danych i sieci rozległe. Audytor wewnętrzny systemów zarządzania obejmujących normy: zarządzania jakością (ISO 9001), zarządzania środowiskowego (ISO 14001), bezpieczeństwem i higieną pracy (OHSAS 18001), bezpieczeństwem produkcji wartościowej (CWA 14641 – Intergraf) oraz zarządzania zarządzania bezpieczeństwem informacji zgodnie z normą ISO/IEC 27001. Certyfikowany audytor systemów IT (CISA), posiadacz certyfikatu ITIL Foundation. Rzeczoznawca PTI, ekspert PIIT. Dyrektor Operacyjny Trusted Information Consulting Sp. z o.o.

Cyberbezpieczeństwo nie jest tylko dla „jajogłowych"

Cyberbezpieczeństwo nie jest problemem technologicznym, lecz biznesowym. Jak spojrzymy na raporty CERT.PL czy ENISA, to dominującą przyczyną wystąpienia incydentów jest czynnik ludzki. Pośpiech, niedostateczny poziom świadomości czy ułomne procesy wewnętrzne ułatwiają atakującym osiągnięcie swoich celów.

Traktuj to osobiście – to twój problem, ale dasz radę

Praktycznie każda polityka bezpieczeństwa, z którą się spotkałem, deklaruje, że bezpieczeństwo to odpowiedzialność wszystkich pracowników. Niestety, w większości nie rozumieją oni, jaki jest ich faktyczny wpływ na bezpieczeństwo. Nie tylko z punktu widzenia biznesu (działalności zawodowej), lecz również w sferze prywatnej. Pandemia i upowszechnienie pracy zdalnej zatarło w znacznej mierze ten podział. Obydwie te sfery życia wzajemnie się przenikają, więc warto to wykorzystać, aby faktycznie zaangażować wszystkich w cyberbezpieczeństwo.

Więcej marchewki, mniej kija

Szkolenia powinny budować świadomość potencjalnych korzyści, odnoszonych również w sferze prywatnej, powinny być motywujące, a nie odstraszające. Promujmy przyjęcie właściwej postawy, a nie straszmy wysokością grożącej kary. Inaczej nikt, z obawy przed potencjalnymi problemami, nie zgłosi podejrzenia wystąpienia incydentu.

Wyeliminuj fałszywe poczucie bezpieczeństwa

Często myślimy, że przecież to tylko „może" się wydarzyć, ale nie musi. Dlaczego akurat ma to spotkać mnie, przecież nie jesteśmy „najgorszą firmą"? Wypełniamy tabelki samooceny i zawsze wychodzi wspaniale, więc czym się przejmować? Były przecież audyty, wiszą certyfikaty, ktoś mówił o analizie ryzyka (są strasznie zapracowani, podobno ledwo się zmieściła w Excelu).

Niestety, są to często pozory. Dowody na „dochowanie należytej staranności", które przyjmują formę fasadową.

Ryba psuje się od głowy

To organ zarządzający i podlegli mu menedżerowie powinni być najbardziej zainteresowani oceną faktycznej sytuacji, i na tej podstawie powinni podejmować odpowiednie działania. Tu nie chodzi o puste deklaracje, lecz o zaangażowanie w działanie i zapewnienie odpowiednich środków (zasobów) do realizacji jasno postawionych celów. To najwyższe kierownictwo powinno pierwsze uczestniczyć we wszystkich wydarzeniach istotnych dla cyberbezpieczeństwa (patrz wymaganie *5.1 Przywództwo i zaangażowanie* w normie ISO/IEC 27001).

KISS lub po polsku BUZI[1]

Podobno „wszystko można zrobić prościej, ale nie prościej niż można"[2]. Ktoś inny przywoła tzw. brzytwę Ockhama – „nie należy mnożyć bytów ponad potrzebę[3]". Niestety, w praktyce powstają polityki i procedury, które są kopią norm i nie wnoszą nic do rozwiązania oprócz zniechęcenia odbiorcy. Powstają rozwiązania nieergonomiczne, zatem nieużyteczne (np. bardzo skomplikowane, wieloetapowe procedury angażujące dziesiątki osób). Powstają procedury pełne wyjątków i niedopowiedzeń, służące wyłącznie ochronie partykularnych interesów osób odpowiedzialnych za dany obszar działalności (rozmycie i wyłączenie odpowiedzialności). Dzieje się tak zawsze, gdy liczy się „posiadanie dokumentacji", a nie „skuteczność zabezpieczeń". Dokumentację po prostu łatwo rozliczyć – nawet jeżeli tylko z liczby stron.

Pytajmy dlaczego

Problem dobrze zdefiniowany jest już w połowie rozwiązany[4]. Nie bójmy się zadawać pytań. Rozmawiajmy i starajmy się znaleźć wspólny język. Szanujmy się wzajemnie. Pokazujmy na przykładach[5]. Bądźmy cierpliwi (nie każdy nauczy się wszystkiego w ciągu jednego dnia – nie od razu Kraków zbudowano). Bądźmy czasem „adwokatem diabła"[6] i nie dajmy się zwieść rutynie. Jeśli my tego nie zrobimy, to zweryfikuje to za nas życie w sposób bardziej bolesny. Incydent cyberbezpieczeństwa w obecnych czasach nie jest naprawdę niczym wyjątkowym.

Konkluzja

Pamiętajmy, najbardziej niebezpieczną polityką bezpieczeństwa, znacznie bardziej niebezpieczną niż jej nieposiadanie, jest tzw. papierowy system zarządzania bezpieczeństwem. Daje on jedynie fałszywe poczucie bezpieczeństwa. Cyberbezpieczeństwo, aby było skuteczne, powinno być elementem kultury organizacyjnej, a nie tylko zbiorem dokumentów. Jak to sprawdzić w praktyce? Wystarczy tylko obserwować, co się dzieje, gdy „żadnego bezpiecznika nie ma w pokoju".

---

1 KISS – ang. Keep It Simple Stupid; BUZI – pol. Bez Udziwnionych Zapisów Idioto.

2 Sentencja przypisywana Albertowi Einsteinowi.

3 łac. *Entia non sunt multiplicanda praeter necessitatem* – faktycznie nie pochodzi od Ockhama, lecz od siedemnastowiecznego niemieckiego filozofa Johannesa Clauberga.

4 Powiedzenie przypisywane Charlesowi Ketteringowi, który uzyskał 186 amerykańskich patentów. Jest wynalazcą m.in. elektrycznego rozrusznika samochodowego, inkubatora dla wcześniaków i pionierem w zastosowaniu magnetyzmu w diagnostyce medycznej.

5 *Powiedz mi a zapomnę, pokaż mi a zapamiętam, pozwól mi wziąć udział, a zrozumiem* – Konfucjusz.

6 Osoba, która celowo wynajduje negatywne cechy lub niekorzystne strony czegoś, aby zmobilizować innych do lepszego rozwiązania określonego problemu.