aut. Artur Marek Maciąg 25.09.2018

BUDOWANIE ŚWIADOMOŚCI CYBERBEZPIECZEŃSTWA TO SYZYFOWA PRACA [KOMENTARZ]

Cyberbezpieczeństwo i edukacja to procesy, które się nie zazębiają. W efekcie otrzymujemy wytyczne, dobre praktyki, polityki, procedury, instrukcje, algorytmy działania, które są sporządzane jakby dla maszyn. Język naturalny ma niewiele z tym tworem wspólnego, podobnie jak z równaniami matematycznymi. Dlatego powszechnie uznaje się, że nauki ścisłe są trudne do przyswojenia. Zupełnie jak współczesne cyberbezpieczeństwo.

Bezwzględnie problemem w cyberbezpieczeństwie jest człowiek i jego skłonność do popełniania błędów, chodzenia na skróty, szukania wygodnych rozwiązań, braku czasu na zastanowienie. Jest też stres, a dodatkowo wstyd związany z powtarzaniem błędów. Jest i pogłębiający się lęk niedoinformowania w dobie gdy informacja jest najcenniejszym surowcem. Tak wygląda „czynnik ludzki" czyli słabe ogniwo w procesie cyberbezpieczeństwa.

Budowanie świadomości cyberbezpieczeństwa jak i uogólniając kultury bezpieczeństwa grupy ludzi czy całego narodu jest iście syzyfową pracą. Nie tylko cały czas pod górkę, z uwagi na zmieniające się warunki technologiczne, to jeszcze nieuchwytny przez nieprzewidywalne zachowania użytkowników w reakcji na zaawansowaną technologię. Phishing, sexting, exhibicjonizm danych, gadżeciarstwo Internet Rzeczy eksplodowały z siłą nie do przewidzenia przez ekspertów technologicznych, zaskoczyło nawet socjologów, dając im fascynujące pole do badań ludzkiej natury, która wydaje się, że zerwała się ze smyczy cywilizacji.

Problem nie byłby tak dotkliwy gdyby dotyczył jednostek. Z uwagi jednak na charakter usług cyfrowych i przepływu informacji oraz sposobu podejmowania indywidualnych decyzji – dotyczy każdej strefy życia społecznego. Kłopot stał się poważnym (choć niedocenianym) zagrożeniem dla państwa, od infrastruktury krytycznej (obsługiwanej przez ludzi) po stabilność i integralność narodu oraz ład społeczny.

Państwo reaguje strategią cyberbezpieczeństwa, której jednym z elementów jest edukacja. Niestety element ten nie został jeszcze doprecyzowany. Grupa robocza do spraw cyberbezpieczeństwa przy Ministerstwie Cyfryzacji dyskutuje kierunki akcji edukacyjnych. Mowa o odpowiedzialności zarządu firmy za proces edukacji cyberbezpieczeństwa, nawet karnej. Poruszona jest kwestia programu edukacji. Dostrzeżono również kwestię problemu braków kadrowych i luk kompetencji istniejącej kadry. I tutaj wychodzi problem edukacji cyberbezpieczeństwa a raczej bezpieczeństwa informacji w pełnej krasie.

Bezpieczeństwo informacji, praktycznie zagarnięte obecnie przez termin cyberbezpieczeństwa dotyczy problemu przekazania informacji pomiędzy co najmniej dwiema uprawnionymi do tej informacji osobami. Tylko po co? I dlaczego? Po co zwykły obywatel ma znać podstawy

bezpieczeństwa informacji zapisanej na dowolnym nośniku (nie tylko cyfrowym)? Czy przyda mu się to w życiu bardziej niż $E=mc^2$, czy Twierdzenie Pitagorasa? Osoby odpowiedzialne za edukację w naszym kraju są zgodne – nie, nie przyda się. A może nie mają zdania? Tak czy inaczej, ani dzieci, ani młodzież, ani nawet dorośli nie poznają podstaw bezpieczeństwa informacji w systematyczny sposób. I nie mowa tutaj o sławnej triadzie bezpieczeństwa: poufność, dostępność i integralność. Nota bene, ze zrozumieniem jej aspektów eksperci mają nie lada problemy, choć recytują ją nawet obudzeni w środku nocy. Istnieje coś bardziej podstawowego i jednocześnie naturalnego dla każdego człowieka: ciekawość.

Edukacja to naturalny proces wykorzystujący ciekawość do zdobycia doświadczenia i wiedzy wspomagającej to doświadczenie. System edukacji 5E o którym eksperci od cyberbezpieczeństwa albo nie wiedzą, albo nie chcą wiedzieć opiera się na naturalnej ciekawości, bardzo silnym bodźcu motywującym każdego z nas. System ten zawiera się w pięciu słowach: Engage (nawiąż do wcześniejszych doświadczeń), Explore (pokaż prosty przykład, praktyczny i czytelny), Explain (poznaj jak jest rozumiany, popraw, zdefiniuj co potrzeba), Elaborate (pozwól rozwinąć przykład szerzej, dopuść eksperymenty i dyskusję), Evaluate (oceń czy mechanizm działa poprawnie, czy wnioski są spójne i zgodne). Czy takie są właśnie Twoje doświadczenia z edukacją dotyczącą cyberbezpieczeństwa?

Nie czekając na państwo i jego mechanizmy, słowniki i katalogi umiejętności, możesz znacząco wzmocnić swoją wiedzę i umiejętności dotyczące cyberbezpieczeństwa. Tu i teraz. Użyj swojej ciekawości i posłuż się literackimi „sześcioma pokornymi sługami" ich imiona to: Kto i Dlaczego, oraz Co, Jak, Gdzie i Kiedy? Pytaj i kwestionuj wszytko co nie jest dla Ciebie zrozumiałe. W tym również tak zwane dobre praktyki cyberbezpieczeństwa. Co to za dobra praktyka, gdy nie może być skutecznie zastosowana, lub wymaga wiedzy i zdolności szpiega na terenie wroga? To właśnie tak proste, jak wygląda.

Czytasz informację która jest zaskakująca? Sprawdź źródło, a jak nie możesz, to ją zignoruj. Nie potrzebujesz śmieci, które ktoś podrzucił na Twoje podwórko. Informacja w swojej naturze zostaje „z tyłu głowy" i jeszcze podejmiesz decyzję bazując na czymś, co nie tylko nie jest prawdą, ale celowo ma wpłynąć na Twoje życie. Przekazujesz taką informację dalej kliknięciem? Narażasz innych.

Dostajesz e-maila od nieznanej osoby, lub z absurdalną prośbą, z załącznikiem którego nie powinno być? Zignoruj, albo lepiej – wyślij do analizy specjalistów.

Na naukę nigdy nie jest za późno. Świat się zmienia a my razem z nim, warto zrobić to razem. Tak to powinno być dostrzegane przez państwo – edukacja to wspólny wysiłek wszystkich: państwa z użyciem budżetu i mechanizmów komunikacji społecznej oraz procesów edukacji powszechnej, specjalistów w zakresie weryfikacji oczekiwań do możliwości i każdego, bez różnicy, bo bez własnego przykładu, marny to trud i strata środków.