# Niekompetentne cyberbezpieczeństwo

## Dlaczego edukacja jest naszą najlepszą bronią przeciwko cyberprzestępstwom.

Clare Naden

fot. © Beenis / Adobe Stock

Internet okazał się jednym z największych wygranych zeszłorocznej pandemii; ruch w sieci i liczba transakcji osiągnęły w 2020 r. bezprecedensowe poziomy. Nic dziwnego, że wraz z tym wzrosła też liczba ataków i szkodliwej aktywności. Według sekretarza generalnego INTERPOL-u, Jürgena Stocka, „cyberprzestępcy rozwijają się i zwiększają liczbę ataków w alarmującym tempie, wykorzystując strach i niepewność wywołane przez niestabilną sytuację społeczną i gospodarczą spowodowaną przez COVID-19".

Dzieje się to w chwili, gdy według szacunków nawet 3,5 miliona miejsc pracy w obszarze cyberbezpieczeństwa pozostanie nieobsadzonych – to zła wiadomość. Czy właśnie przegrywamy bitwę? Podnoszenie kwalifikacji osób już pracujących w cyberbezpieczeństwie i zachęcanie nowych do zatrudnienia się w tej branży jest naszą najlepszą obroną, ale programy nauczania są fragmentaryczne i niewystarczające.

Spotykamy się ze światowej sławy specjalistą ds. bezpieczeństwa IT, drem Edwardem Humphreysem, aby porozmawiać z nim o zagrożeniach związanych z niedoborem umiejętności cybernetycznych i potencjalnych konsekwencjach tego zjawiska dla gospodarki i społeczeństwa. Doktor Humphreys zasiada w wielu komitetach prowadzonych wspólnie przez ISO i IEC, w tym we Wspólnym Komitecie ISO/IEC JTC 1 *Information technology*, podkomitecie SC 27 *Information security, cybersecurity and privacy protection*, który opublikował ponad 200 norm, a kolejnych 77 opracowuje. Ekspert w swojej dziedzinie, często cytowany jako „ojciec" rodziny norm ISO/IEC 27001 dla systemów zarządzania bezpieczeństwem informacyjnym.

## Cyberbezpieczeństwo to ciągła walka, a zapotrzebowanie na cybertalenty stale rośnie i wciąż przewyższa podaż. Jak ta sytuacja wygląda dzisiaj?

Warto przytoczyć starożytną mądrość dotyczącą strategii wojennej. Ten cytat jest dziś dość często używany w różnych kontekstach edukacyjnych i szkoleniowych dla profesjonalistów z wielu dziedzin, w tym zarządzania, negocjacji biznesowych i oczywiście cyberbezpieczeństwa.


fot. © TaweeW.asurut / Adobe Stock

fot. © RoBird / Adobe Stock

„Poznaj dobrze wroga i poznaj dobrze siebie, a w stu bitwach nie doznasz klęski. Jeśli ignorujesz wroga, a dobrze znasz tylko swoje siły, masz równe szanse na zwycięstwo i przegraną. Jeśli nie liczysz się ani z siłą wroga, ani też nie znasz własnej siły, możesz być pewny, że poniesiesz klęskę w każdej bitwie[1]".

Im więcej mamy informacji o naszych mocnych i słabych stronach oraz o naszych wrogach, tym lepiej jesteśmy przygotowani. Powinniśmy zdobywać informacje o tym, kim jest nasz wróg, dlaczego, kiedy, jak i co może zaatakować oraz co chce na tym zyskać. Jeśli dobrze znamy siebie i naszego wroga, mamy duże szanse, żeby wygrać bitwę.

Załoga, która jest świadoma kwestii cyberbezpieczeństwa, w skład której wchodzą wykwalifikowani specjaliści i dobrze poinformowani pracownicy, stawia nas na dobrej pozycji. Oznacza to inwestowanie czasu i pieniędzy w edukację, szkolenia i podnoszenie świadomości w zakresie cyberbezpieczeństwa. Organizacje z potencjalnie zwycięską strategią w cyberbezpieczeństwie to takie, które mają skuteczny system zarządzania ryzykiem i wykwalifikowaną w kierunku cyberbezpieczeństwa kadrę. Te dwa elementy łącznie umożliwiają organizacji ocenę jej mocnych i słabych stron, aby lepiej wytrzymała atak.

## Niedobór wykwalifikowanych ekspertów w tej dziedzinie. Dlaczego?

Technologia ciągle się zmienia, więc personelowi z branży trudno jest nadążyć, a często potrzebna jest specjalistyczna wiedza, której zdobycie wymaga czasu. Według Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) producenci i inne organizacje korzystające z rozwiązań Przemysłu 4.0 i Internetu Rzeczy często nie mają czasu na odpowiednie przeszkolenie pracowników, co naraża je na potencjalne ryzyko. Co więcej, dostępne szkolenia są niewystarczające i drogie.

W ostatnich latach eskalacja cyberataków spowodowała, że organizacje spieszą się bardzo z rekrutacją wykwalifikowanych specjalistów, przez co rynek został wydrenowany z talentów. Pilną potrzebę podjęcia działań pogorszyło pojawienie się COVID-19 i sygnały alarmowe wynikające z dramatycznego wzrostu udanych ataków. Kształcenie i szkolenie w zakresie cyberbezpieczeństwa nie nadążają w budowaniu wykwalifikowanej kadry.

[1] Sun Tzu, „Sztuka wojny, czyli trzynaście rozdziałów", str. 27, https://www.lazarski.pl/fileadmin/user_upload/dokumenty/student/Sun_Tzu_sztuka_wojny.pdf.

Przyczyny tego niedoboru są liczne i różnorodne. Na poziomie edukacyjnym (uniwersytet, szkoła wyższa) zainteresowanie cyberbezpieczeństwem jako kierunkiem kształcenia stale rośnie, ale liczba absolwentów wciąż nie odpowiada zapotrzebowaniu. Kształcenie i szkolenie wysoko wykwalifikowanych specjalistów wymaga czasu tak samo jak zdobycie praktycznego doświadczenia zawodowego. Tymczasem inwestycje w szkolenia z zakresu cyberbezpieczeństwa zostały poważnie ograniczone, ponieważ zredukowano budżety na wydatki niezwiązane bezpośrednio z zyskami i uzyskiwaniem przychodów.

## Co to oznacza dla naszej przyszłości, jeśli nic więcej nie zostanie zrobione?

Ogólnoświatowy niedobór wykwalifikowanego personelu cybernetycznego ma bezpośredni i znaczący wpływ na organizacje i ich zdolność do (cybernetycznej) samoobrony. A to stanowi poważne zagrożenie dla ogólnego dobrobytu gospodarczego kraju, a co za tym idzie, również społeczeństwa.

Problem obejmuje co najmniej trzy obszary:

- wykwalifikowanych specjalistów do zarządzania, administrowania i wspierania bezpieczeństwa i działalności organizacji;
- wykwalifikowanych cyberinżynierów do projektowania systemów bezpieczeństwa oraz tworzenia bezpiecznego oprogramowania i narzędzi;
- ogólną świadomość dotyczącą cyberbezpieczeństwa na każdym poziomie organizacji tak, aby każdy miał podstawową wiedzę na temat zagrożeń i ryzyka oraz tego, co to oznacza w kontekście pełnionej przez każdą osobę funkcji.

Zwiększające się wykorzystanie Internetu i usług online, wprowadzanie nowych technologii i szybko zmieniające się środowisko cyfrowe potęgują potrzebę dobrego i jeszcze lepszego cyberbezpieczeństwa. Rozpaczliwy niedobór specjalistów z umiejętnościami cybernetycznymi z pewnością opóźni postęp w osiąganiu odpowiedniej i skutecznej ochrony.

Jeśli globalny niedobór wykwalifikowanej kadry w dziedzinie cyberbezpieczeństwa będzie się utrzymywał, organizacjom trudno będzie zwyciężyć w tej bitwie. Perspektywą przyszłości stanie się większe narażenie na cyberataki skutkujące większymi stratami finansowymi, większymi zakłóceniami w działalności, przerwami w świadczeniu usług i łańcuchów dostaw, naruszaniem prywatności i bezpieczeństwa osobistego oraz wieloma innymi skutkami.


fot. © RoBird / Adobe Stock

fot. © Song_about_summer / Adobe Stock

## Podejmuje się jakieś działania, żeby zachęcić talenty cybernetyczne do podnoszenia kwalifikacji?

ENISA opowiada się za łączeniem wiedzy o bezpieczeństwie technologii informacyjnych (IT) z wiedzą dot. technologii operacyjnych (OT) oraz za dalszymi szkoleniami i edukacją. Budowanie zdolności uczyniła kluczowym celem swojej nowej strategii; podejmuje też wiele działań podnoszących świadomość wśród konsumentów, aby promować bezpieczniejsze zachowania w Internecie. Upowszechnia także i analizuje edukację w zakresie cyberbezpieczeństwa, aby zaradzić deficytowi zawodowemu w tej dziedzinie, bo stanowi to problem zarówno dla rozwoju gospodarczego, jak i dla bezpieczeństwa narodowego.

W krajach takich jak Stany Zjednoczone i Wielka Brytania prowadzonych jest wiele kampanii promujących wiedzę na temat kariery zawodowej w dziedzinie bezpieczeństwa cybernetycznego, ale to nie są skoordynowane działania i nie ma tu żadnej harmonizacji na poziomie międzynarodowym.

Niektóre kraje ustanowiły programy, które biorą pod uwagę ten problem. Obejmują one krajowe kampanie zachęcające uniwersytety, szkoły i organizacje szkoleniowe do promowania wyboru cyberbezpieczeństwa jako dziedziny studiów. Na przykład w Kanadzie i Wielkiej Brytanii cyberedukację zaczyna się wprowadzać do szkół dla dzieci w wieku od 8 lat. To dobra wiadomość, biorąc pod uwagę, że musimy budować przyszłe pokolenia talentów z umiejętnościami cybernetycznymi.

## Obecnie pracujesz nad nową normą dotyczącą edukacji w branży cyberbezpieczeństwa. Czy to pomoże, a jeśli tak to jak?

Jedna z naszych grup roboczych rozpoczęła opracowywanie raportu technicznego dotyczącego edukacji i szkoleń w zakresie cyberbezpieczeństwa. Kiedy zostanie opublikowany, określi, dlaczego, co i jak należy zrobić w zakresie edukacji i szkoleń z cyberbezpieczeństwa, aby poprawić obecną sytuację.

Raport techniczny dostarczy nam więcej danych o tym, dlaczego edukacja i szkolenia w zakresie cyberbezpieczeństwa są takie ważne i jak są niezbędne do tworzenia dobrze poinformowanej i kompetentnej kadry pracowniczej, która może chronić biznes i społeczeństwo. Raport wyjaśni również, dlaczego edukacja w zakresie cyberbezpieczeństwa musi być strategicz-

nym priorytetem rozwoju pracowników w organizacjach, agendach rządowych i we wszystkich sektorach biznesu.

Przewodnik będzie zawierał listę dostępnych inicjatyw i programów krajowych dotyczących kształcenia formalnego, szkoleń zawodowych, norm i wytycznych. Dzięki temu można będzie go wykorzystywać do identyfikacji obszarów wymagających poprawy i dalszego rozwoju. Będzie również opisywał specjalistyczne obszary edukacji w zakresie cyberbezpieczeństwa, które mają kluczowe znaczenie do zapewnienia skutecznej ochrony cybernetycznej.

## Dla kogo jest ten dokument i kiedy będzie można z niego skorzystać?

Dokument w założeniu ma być przydatny każdemu, kto zajmuje się cyberbezpieczeństwem: użytkownikom, dostawcom, osobom certyfikującym, decydentom i regulatorom, pedagogom, konsumentom, sprzedawcom i producentom. Spodziewamy się, że zostanie opublikowany pod koniec 2021 r. lub na początku 2022 r.

## Co organizacje mogą zrobić w międzyczasie, aby się chronić?

Jednym z najważniejszych działań, jakie organizacje muszą przedsięwziąć, to pełne zrozumienie zagrożeń, przed jakimi stoją oraz zastosowanie podstawowych mechanizmów kontrolnych w celu złagodzenia tych zagrożeń. Norma ISO/IEC 27002 *Information technology – Security techniques – Code of practice for information security controls* zawiera zestaw mechanizmów kontrolnych wywodzących się z najlepszych praktyk branżowych; umożliwia to dowolnej organizacji budowę zdolności zwalczania zagrożeń dzięki lepszemu zrozumieniu własnych potrzeb, o czym wspominałem na początku. Im więcej się wie na temat możliwych ataków, a także własnych słabości, tym łatwiej jedne i drugie zneutralizować. Mądrość Sun Tzu ze „Sztuki wojny" jest dziś tak samo aktualna, jak wtedy, gdy została spisana po raz pierwszy.

*Oprac. P. M.*
*www.iso.org*

fot. © Song_about_summer / Adobe Stock