Cyberdefence 24

aut. Szymon Palczewski 20.08.2019

CYBERATAK JAK BROŃ JĄDROWA? JEDNO KLIKNIĘCIE NIESIE SPUSTOSZENIE

Na całym świecie wzrasta niepokój związany z napięciami między głównymi mocarstwami oraz rosnącym zagrożeniem możliwości wykorzystania broni nuklearnej. Jednak wiele osób nie zdaje sobie sprawy z faktu, że cyberatak może być równie niszczycielski, jak bomba jądrowa. Hakerzy już dzisiaj rozwijają swoje możliwości w tym kierunku – informuje serwis The Conversation.

Stany Zjednoczone i Rosja wycofały się z układu o całkowitej likwidacji pocisków rakietowych średniego zasięgu. Jednocześnie pracują nad nowymi rodzajami broni nuklearnej. Korea Północna prowadzi kolejną serię testów pocisków rakietowych, a napięcia w Iranie eskalują na cały region. To wszystko sprawia, że wzrasta zagrożenie związane z możliwością realnego użycia broni masowego rażenia (BMR). Według ekspertów należy oczekiwać nowego wyścigu zbrojeń na wzór zimnej wojny - pisze na łamach The Conversation Jeremy Straub.

Problem ten jest powszechnie znany. Jednak niewielu jest świadomych, jakie skutki może mieć zaawansowany cyberatak. Obecnie istnieją twarde dowody, że hakerzy umieścili złośliwe oprogramowanie w amerykańskich systemach energetycznych i innych sektorach, które w każdej chwili może zostać użyte. Z drugiej strony Amerykanie przeprowadzili podobne operacje wymierzone w swoich wrogów - twierdzi Straub.

Jak podaje The Conversation, cyberatak może spowodować ogromne straty, w tym masowe obrażenia lub utratę życia ludności, zbliżone w swojej liczbie do broni nuklearnej. W tym miejscu należy podkreślić, że użycie bomby atomowej powoduje natychmiastową śmierć w najbliższej odległości od wybuchu. Z kolei jeśli chodzi o cyberatak jest to proces znacznie bardziej złożony i powolny. Ludzie mogą tracić życie w wyniku głodu, braku energii, ciepła lub wypadków samochodowych. Skala w tym przypadku jest praktycznie nieograniczona.

Wzajemne gwarantowane zniszczenie

Problemem jest również sama doktryna. Obecnie istnieje wiele regulacji ograniczających możliwość wybuchu wojny nuklearnej w przeciwieństwie do cyberwojny, która nie jest ściśle uregulowana prawem. W tym miejscu należy wyróżnić na przykład koncepcję „wzajemnego gwarantowanego zniszczenia”. Mówi ona, że żaden kraj nie powinien użyć swojej broni atomowej w stosunku do innego państwa atomowego. Podejście to opiera się na zasadzie wzajemnej destrukcji – wystrzelenie pocisków spowoduje odpowiedź wroga, który w reakcji na zagrożenie użyje swojego arsenału, co spowoduje zniszczenie obu państw - informuje The Conversation.

W cyberprzestrzeni nie ma takich ograniczeń. Wynika to z faktu, że o wiele łatwiej jest ukryć źródło cyberataku. Co więcej, cyberwojna może rozpocząć się od małego incydentu, jak zainfekowanie pojedynczego telefonu lub innego urządzenia. Oczywiście cyberprzestępcy mogą od razu ukierunkować swoje działania na większe cele - twierdzi Straub.

Cyberatak jak broń atomowa

Istnieją trzy podstawowe scenariusze rozwoju cyberataku, który może być równie niebezpieczny, jak broń jądrowa - pisze Straub na łamach The Conversation. Po pierwsze, napięcie może zacząć się od małego incydentu, na skutek czego służby wywiadowcze jednego państwa kradną, usuwają lub manipulują danymi wojskowymi innego kraju. Wykryta działalność doprowadzi do odwetu, który może rozszerzyć się na inne działania, doprowadzając do ogromnych szkód.

W drugiej sytuacji aktor państwowy lub organizacja terrorystyczna może przeprowadzić niszczące cyberataki na skalę masową, ukierunkowując działania w kilka obiektów o znaczeniu krytycznym równocześnie. Atrakcyjnym celem są z pewnością podmioty sektora energetycznego oraz uzdatniania wody.

Trzeci scenariusz jest najbardziej niepokojący. Mówi on o możliwości wystąpienia pomyłki. Błędy ludzkie lub mechaniczne bardzo często stanowią ogromne zagrożenie, którego nikt się nie spodziewa. Wystąpienie takiej sytuacji w cyberprzestrzeni może doprowadzić do ogromnej katastrofy, która rozprzestrzeni się na inne podmioty lub regiony.

Obrona przed zagładą

Podobnie jak nie ma sposobu, aby całkowicie zabezpieczyć się przed atakiem nuklearnym, tak cyberataki są bardzo trudne do odparcia. Istnieją jedynie sposoby na zmniejszenie niszczycielskich skutków incydentów - pisze The Conversation.

Po pierwsze, rządy, firmy i zwykli ludzie muszą zabezpieczyć swoje systemy, aby uniemożliwić hakerom uzyskanie do nich dostępu. W ten sposób cyberprzestępcy nie będą mogli skutecznie wykorzystać sieci do bardziej zaawansowanych działań.

Systemy krytyczne muszą być znacznie bardziej bezpieczne. Jedna z przeprowadzonych przez specjalistów analiz wykazała, że tylko około jedna piąta firm używających komputerów do sterowania maszynami przemysłowymi w USA monitoruje swój sprzęt w celu wykrycia potencjalnych ataków. Prawie trzy czwarte firm energetycznych doświadczyło pewnego rodzaju ingerencji w sieć w poprzednim roku – przypomina serwis The Conversation.

Po trzecie, systemów nie da się zabezpieczyć bez wykwalifikowanego personelu. Obecnie prawie jedna czwarta wszystkich miejsc pracy związanych z cyberbezpieczeństwem w Stanach Zjednoczonych jest nieobsadzona. Jeden z rekruterów wyraził zaniepokojenie podkreślając, że niektóre stanowiska są zajmowane przez osoby, które nie mają odpowiednich kwalifikacji. Rozwiązaniem jest prowadzenie większej ilości szkoleń oraz edukacja, aby nauczyć ludzi potrzebnych umiejętności.