PRZYSZŁOŚĆ CYBERPRZESTĘPCZOŚCI [RAPORT]

W perspektywie najbliższych kilkunastu lat każde dotychczas znane nam przestępstwo stanie się cyberprzestępstwem – to teza najnowszego raportu opublikowanego przez Infuture Hatalska Foresight Institute pt. *Future of Crime* z udziałem ekspertów m.in. Atende oraz Cisco Poland. W raporcie prezentowane są zagrożenia „dzisiaj", „jutro" i „pojutrze" – od ataków na infrastrukturę krytyczną, po hakowanie genów i tzw. mindreading.

Jednym z najważniejszych aktualnie trendów technologicznych omawianych w raporcie jest sztuczna inteligencja (ang. AI, artificial intelligence), a właściwie uczenie maszynowe (ang. machine learning). Technologia AI jest tzw. technologią podwójnego wykorzystania - może być wykorzystana w sposób pozytywny, jak i negatywny (np. dron może dostarczać paczki, ale i być wykorzystywany jako autonomiczna broń).

> *Mówi się, że w kolejnych latach większość ataków hakerskich dotyczących infrastruktury informatycznej wykonywana będzie przez automaty lub boty - za około 5-10 lat około 70% zarobku hakerskiego będzie pochodziło właśnie z tego typu źródeł. Pojawia się tu problem odpowiedniego zabezpieczenia systemów. Jeśli atak był automatyczny, to i odpowiedź na niego również powinna być automatyczna*
>
> Jakub Jagielak, Cyber Security Business Development Manager, Atende S.A

Zaczynamy mówić o predictive security, czyli momencie, gdy technologia pomoże wykrywać pewne miejsca, pliki, działania lub osoby, które szykują się do popełnienia cyberprzestępstwa. Przykładem są miejsca w Internecie; domeny, których zachowanie oznacza, że próbują się ukryć- dodaje Łukasz Bromirski, Dyrektor ds. Technologii, Cisco Poland.

Według opinii ekspertów już dzisiaj najbardziej newralgicznym punktem wśród cyberzagrożeń jest infrastruktura krytyczna (sieci energetyczne, wodociągowe, stacje paliw itp.) – zarówno pod względem prawdopodobieństwa wystąpienia jak i skali jego negatywnego wpływu. Znaczący impuls do postrzegania masowego blackoutu jako realnego zagrożenia dały cyberataki podczas toczącej się wojny rosyjsko-ukraińskiej na ukraińską sieć energetyczną w 2015 r., które spowodowały przerwy w dostawach prądu dla kilkuset tysięcy osób.

W ciągu najbliższych lat najbardziej narażone na ataki cyberprzestępców są także sektory finansowy i medyczny. Podczas gdy poziom zabezpieczeń stosowanych w bankach jest stosunkowo wysoki, w branży medycznej sytuacja wygląda zupełnie inaczej.

W Polsce papierowa informacja o pacjentach nigdy nie była dobrze zabezpieczona, dostęp do niej był łatwy [...] Teraz takie podejście przenosi się także na wersję elektroniczną. I nikt się tym specjalnie nie przejmuje. W zeszłym roku dane medyczne i backupy z jakiegoś szpitala zostały dodane na serwer, który był publicznie dostępny. To takie typowe: „A, wrzućmy te dane gdzieś tam" - mówi Tomasz Judycki, członek zarządu Atende Medica z Grupy Atende.

Eksperci zwracają uwagę na rewolucję w bezpieczeństwie IT wywołaną przez Internet Rzeczy. Gartner szacuje, że do 2020 r. urządzeń podłączonych do sieci będzie ponad 25 mld i jest to jedna z najostrożniejszych estymacji. To z kolei każe myśleć o bezpieczeństwie już na etapie projektowania systemów.

Paweł Pisarczyk, prezes spółek Atende Software i Phoenix Systems z Grupy Atende, architekt Phoenix RTOS - systemu operacyjnego czasu rzeczywistego przeznaczonego dla urządzeń IoT podkreśla: *W większości urządzenia starszej generacji, które będą musiały teraz być zamienione na urządzenia inteligentne, czyli te podłączane do internetu i komunikujące się, były projektowane w ten sposób, że projektant wybierał układ scalony jeden, drugi, trzeci i dopisywał mały kawałek oprogramowania, który miał zapewnić między innymi bezpieczeństwo informatyczne systemu. Na przykład liczniki energii elektrycznej projektowało się w ten sposób. W tej chwili sposób projektowania takich urządzeń musi się drastycznie zmienić. Podejście, w którym ignoruje się bezpieczeństwo podczas projektowania urządzenia na rzecz uproszczenia konstrukcji, będzie skutkowało tym, że internet rzeczy będzie niebezpieczny. Trzeba coś z tym zrobić.*

Eksperci zgadzają się, że do ochrony przed atakami technologia nie wystarczy – trzeba także edukować ludzi i zadbać o odpowiednie procesy.

Mamy problem dotyczący pracowników, którzy chcąc sobie ułatwić pracę, często korzystają z aplikacji czy usług z chmury, które nie są rekomendowane pracownikom przez dział IT danej firmy. Przykładem jest zainstalowanie aplikacji Dropbox, by móc wspólnie wymieniać się większymi plikami. Tego typu problem można nazwać Shadow IT – mówi Łukasz Bromirski z Cisco Poland.

Akurat ataki DDoS (distributed denial of service) są tak rozpowszechnione, bo ludzie nie aktualizują oprogramowania na komputerach i innych urządzeniach. Dla przykładu, kamerki internetowe są szczególnie atrakcyjnym celem ataku - są ciągle podłączone do zasilania i internetu, mogą atakować dzień i noc. Niewielkie spowolnienie w działaniu tych urządzeń nawet nie zostanie zauważone. Łatwo je przejąć, połączyć w botnet i wykorzystywać w dowolnym, przestępczym celu – dodaje Przemysław Frasunek, specjalista z zakresu bezpieczeństwa systemów i kryminalistyki cyfrowej (z wszechstronną wiedzą na temat technik hakerskich) w Atende Software z Grupy Atende. Inżynierowie Atende Software stworzyli redGuardian - usługę świadczoną w chmurze, której przeznaczeniem jest ochrona przed atakami DDoS, która daje możliwość przetwarzania pakietów sieciowych powyżej 100 milionów na sekundę na pojedynczym serwerze klasy PC.

W prezentowanym raporcie, świadomość cyberzagrożeń wśród firm została przez ekspertów oceniona głównie jako słaba lub średnia. Przykładem jest era podłączonych do sieci samochodów.

Mimo szacunków, że podłączonych samochodów będzie coraz więcej (380 mln na drogach do 2021 r.), firmy ubezpieczeniowe - jak wynika z badań przeprowadzonych przez KPMG, nie obawiają się zmian. Aż 95% z badanych menadżerów ubezpieczeniowych, twierdzi, że w ciągu najbliższych 5 lat nic się nie zmieni, a podłączone samochody nie będą miały żadnego wpływu na ich branżę. Dlatego też być może aż 74% badanych potwierdza, że ich firma wcale nie jest przygotowana na te zmiany.

Z kolei w scenariuszach pojutrza raport omawia m.in. technolgie CRISPR (ang. Clustered Regularly-Interspaced Short Palindromic Repeats) – metoda inżynierii genetycznej, pozwalająca na manipulacje

genomem danego organizmu. Edytowanie genów zostało już wpisane przez Biuro National Intelligence w Stanach Zjednoczonych na listę zagrożeń jakie stwarza „broń masowego rażenia i rozprzestrzeniania”. Przytacza także, że w przyszłości cyberprzestępcy będą mogli wykradać nasze myśli. Już dzisiaj naukowcy z MIT Media Lab opracowali urządzenie, za pomocą którego można z 90% dokładnością odgadnąć co chcemy powiedzieć, zanim wypowiemy jakiekolwiek słowo na głos.

Raport powstał w oparciu o wywiady delfickie oraz wyniki ankiet przeprowadzonych wśród najlepszych ekspertów branży IT. Zachęcamy do przeczytania raportu oraz pobrania pełnej, bezpłatnej wersji przez stronę: https://futureofcrime.atende.pl/.