CAŁA INFRASTRUKTURA NA OKU – ITMANAGER

Najgłośniejsze wycieki danych dotyczą największych firm i gigantów technologii. Jednak zagrożenie dotyczy wszystkich organizacji na rynku, także małych i średnich. Od wejścia w życie RODO, ponoszą one taką samą odpowiedzialność prawną jak międzynarodowe korporacje.

Za naruszenia bezpieczeństwa w firmach najczęściej odpowiadają hakerzy, którzy uzyskali nieautoryzowany dostęp do wewnętrznej sieci firmy. Według serwisu Breach Level Index, który monitoruje światowe wycieki danych, osoby spoza organizacji mające złe zamiary (tzw. malicious outsider) odpowiadały za 61,49% wycieków danych od 2013 roku. Z kolei w 23% spraw była to przypadkowa utrata a w 12,06%[1] działanie osoby o złych zamiarach osadzonej wewnątrz firmy.

- Znaczna większość cyberataków wykorzystuje dziury w oprogramowaniu, które pozwalają nieuprawnionym użytkownikom dostać się do systemu – tłumaczy **Szymon Dudek, Dyrektor Działu Oprogramowania w Infonet Projekt SA.** - Dlatego tak istotne jest, aby administratorzy dbali o regularną aktualizację systemów, które mają pod opieką.

Ogarnąć cały system

W przypadku polskich małych i średnich przedsiębiorstw, na kilkadziesiąt lub kilkaset komputerów przypada co najwyżej kilku administratorów. Ich zadania to dbanie o cyberbezpieczeństwo firmy, komfort pracowników oraz działanie infrastruktury bez przerw i awarii.

- We wszystkich tych aspektach największym wyzwaniem jest zapanowanie nad czynnikiem ludzkim. W nawet najszczelniejszym systemie najsłabszym ogniwem jest użytkownik.

Raport firmy Kaspersky Lab zajmującej się cyberbezpieczeństwem wskazuje, że w samym tylko drugim kwartale 2018 roku oprogramowanie Kaspersky zablokowało ponad 962 mln ataków informatycznych prowadzonych z terenów 187 krajów świata. Ponad 351 mln stron zostało uznanych za niebezpieczne i służące do rozprowadzania złośliwego oprogramowania.

- Przestępcy dzięki nowoczesnym technologiom stosują wiele wyrafinowanych technik. Od stosunkowo prostego wyłudzania haseł i wykradania danych, przez przejęcie części mocy obliczeniowej komputera do wydobywania kryptowalut, aż do szyfrowania całego dysku twardego i żądania okupu za przejęte informacje – tłumaczy **Szymon Dudek.**

Portal Cybersecurity Ventures wskazuje, że suma okupów za ransomware (oprogramowanie szantażujące) w 2018 roku przekroczy 8 mld dolarów. Skala problemu rośnie – w 2019 r. statystycznie co 14 sekund jakaś firma będzie celem ataku ransomware. Jeden z najpoważniejszych ataków w historii, WannaCry, rzucił na kolana m.in. FedEx, brytyjski odpowiednik NFZ (NHS) oraz Deutche Bahn[2].

- Dlatego z perspektywy administratorów systemu tak istotne jest, by użytkownicy nie instalowali nieautoryzowanego oprogramowania i nie wchodzili na niegodne zaufania strony internetowe. Śmieszny

wygaszacz lub zestaw czcionek może się dla przedsiębiorstwa zakończyć ogromnymi kosztami – tłumaczy **Dyrektor Działu Oprogramowania.** Jego zdaniem scentralizowane narzędzie do zarządzania infrastrukturą IT jest jedną ze skuteczniejszych odpowiedzi na to wyzwanie.

- Nasz system ITManager pozwala z jednego miejsca zarządzać wieloma aspektami firmowej infrastruktury. Od oprogramowania, które jest zainstalowane na każdym z komputerów, przez nadane uprawnienia użytkowników i co mogą w ich ramach zrobić, aż po strony internetowe i serwisy, z których korzystają – podkreśla **Szymon Dudek z Infonet Projekt SA.** - Dzięki temu możliwe jest określenie najbardziej ryzykownych punktów w organizacji oraz opracowanie polityki uwzględniającej te zagrożenia.

RODOodporni

Odpowiednia polityka jest szczególnie istotna w kontekście RODO, które od maja 2018 roku reguluje kwestię ochrony i przetwarzania danych osobowych obywateli Unii Europejskiej. W przypadku szczególnie dramatycznych nadużyć firmy muszą liczyć się z dotkliwymi karami, nawet do 20 mln euro lub 4% rocznego obrotu firmy.

Z tego względu organizacje starają się tak kształtować uprawnienia pojedynczych użytkowników, aby chronić system przed ich błędami.

- Sednem tego prawa jest opracowanie odpowiednich zasad bezpieczeństwa w firmie. W razie kłopotów pozwalają one wykazać, że zostały podjęte „najlepsze możliwe środki bezpieczeństwa", jakie leżały w zasięgu organizacji – tłumaczy Szymon Dudek. - W tym kontekście narzędzie do scentralizowanego zarządzania infrastrukturą, które pozwala kontrolować wdrożenie takiej polityki, jest nie do przecenienia. Nawet najlepsze procedury nie pomogą, jeśli nie są przestrzegane.

Zoptymalizować licencje

Dzięki skupieniu w jednym miejscu informacji dotyczących oprogramowania wykorzystywanego przez pracowników, możliwe jest sprawniejsze zarządzanie licencjami.

- Dane te dają jasną informację na temat oprogramowania, jakiego pracownik potrzebuje do wykonywania swoich obowiązków. Jeśli pracownik domagał się pakietu biurowego a spędza w nim najwyżej godzinę tygodniowo, być może warto wygasić te licencje dla oszczędności lub przesunąć na inne stanowiska, gdzie mogą się bardziej przydać – tłumaczy ekspert firmy **Infonet Projekt SA.** Podkreśla jednocześnie, że w skali kilkudziesięciu czy nawet kilkuset komputerów oszczędności na abonamencie za pakiet Office mogą być szczególnie odczuwalne.

Podobnie sytuacja, w której pracownicy intensywnie korzystają z narzędzi online lub zamienników programów stosowanych w organizacji, może być sygnałem, że w przedsiębiorstwie potrzebne są zmiany.

- Jaki jest sens utrzymywania narzędzia do zarządzania projektami, jeśli pracownicy wybierają zamiast niego darmową Asanę lub podobny program? - pyta retorycznie **Szymon Dudek.**

Samooptymalizacja

Opcjonalnym komponentem oprogramowania ITManager jest narzędzie do monitorowania aktywności pracowników, które mierzy czas spędzony w konkretnych aplikacjach i witrynach internetowych.

- Całkowicie zrozumiałe jest, że w niektórych branżach i na części stanowisk konieczne jest kontrolowanie czasu spędzanego w poszczególnych programach internetowych. W przypadku ochroniarzy czy nadzorców ruchu utrzymanie skupienia jest szczególnie istotne. Jednocześnie jest to dość monotonna praca a pokusa oderwania się choćby na chwilę jest ogromna – tłumaczy **Szymon Dudek.** – W niektórych sytuacjach taka chwila rozkojarzenia może pociągać za sobą wyjątkowo groźne konsekwencje, w skrajnych sytuacjach nawet może kosztować kogoś życie.

– Z tego względu przygotowaliśmy również moduł, w ramach którego pracodawca uzyskuje informacje na temat aktywności pracownika: kiedy włączył komputer, jak intensywnie z niego korzystał, ile czasu spędził w zainstalowanych aplikacjach Zdaniem ekspertów firmy Infonet Projekt SA jest to istotne zwłaszcza, jeśli pracownik ma za zadanie nadzorować konkretny proces.

- Informacja, że w momencie, gdy popełniony został błąd, pracownik od godziny nie poruszył myszą przy komputerze jest wyraźnym sygnałem, że nie przyłożył się do swojej pracy należycie – podsumowuje **Szymon Dudek, Dyrektor Działu Oprogramowania w Infonet Projekt SA.**

[1] https://breachlevelindex.com/

[2] https://pl.wikipedia.org/wiki/WannaCry