Prezentujemy Wam szósty numer naszego S.M.S.-owego biuletynu bezpieczeństwa komputerowego „Z firewall’a wzięte”.

Spis treści

Wstęp

Przygotowaliśmy dla Was szósty numer naszego biuletynu bezpieczeństwa komputerowego „Z firewall’a wzięte” analizujący zagrożenia 2020 roku. Znów macie możliwość zajrzenia do naszej infrastruktury i przekonania się z jakimi podatnościami mierzymy się codziennie. Zapraszamy również do zapoznania się z pierwszym numerem biuletynu, gdzie szczegółowo opisujemy powody dla, których postanowiliśmy tworzyć takie materiały. Standardowo biuletyn składa się z 3 głównych części – ogólnej analizy statystycznej incydentów w naszej infrastrukturze, analizy przypadku jednego z wybranych przez nas zagrożeń oraz podsumowania całego zebranego przez nas materiału. Na końcu dodaliśmy również sekcję „Poprzednie numery”, co pozwoli Ci łatwo znaleźć wcześniejsze wydania biuletynu.

Numer marcowy jest dla nas wyjątkowy, ponieważ do pomocy w jego przygotowaniu udało nam się namówić dostawcę rozwiązań z dziedziny bezpieczeństwa IT, a mianowicie Fudo Security!. Nasza znajomość z nimi trwa już kilka dobrych lat, bo w ramach Security BSides Warsaw wspierają nas regularnie pod względem merytorycznym oraz marketingowym. Tym razem jednak postanowili dać nam dostęp do testwania swojego rozwiązania Fudo PAM i rzucili nam wyzwanie co takiego uda nam się dzięki niemu złowić na naszym firewall’u. Aby dowiedzieć się, więcej o samym Fudo Security oraz sprawdzić nad czym pracują wpadnijcie na ich profile w social mediach – LinkedIn, Twitter, Facebook. Koniecznie dajcie znać, że przysłało Was S.M.S.!

Chcielibyśmy również zachęcić naszych kolegów z branży do przyłączenia się do naszej inicjatywy i współpracy przy tworzeniu kolejnych wydań biuletynu. Jeśli masz pomysł jak wykorzystać Twój potencjał, pomysł lub produkt w materiale serdecznie zapraszamy

do kontaktu mailowego w celu ustalenia szczegółów: blog@s-m-s.pl.

Mamy nadzieję, że zapoznanie się z materiałem sprawi Ci tyle satysfakcji ile nam sprawiło jego przygotowanie. Zapraszamy również do dyskusji na jego temat we wszystkich dostępnych kanałach – sekcja komentarzy na naszym blogu, nasze profile w social mediach (Facebook oraz Twitter) czy też pod adresem mailowym: blog@s-m-s.pl. Każda opinia na ten temat jest dla nas ważna i pomoże nam ulepszyć kolejne wydania biuletynu.

Miłej lektury!

Ogólna analiza statystyczna incydentów

W celu określenia skali i częstotliwości występowania zdarzeń w infrastrukturze najlepszym będzie przeanalizowanie dostępnych danych statystycznych. Dzięki takiemu zabiegowi będziemy mogli w sposób kompleksowy przedstawić kwestie cyberbezpieczeństwa naszej infrastruktury. Na potrzeby przygotowania tej części materiału wykorzystaliśmy technologię umożliwiającą nam stałe monitorowanie ruchu do naszych serwerów. Pozwoliło nam to wyszczególnić zdarzenia, które zostały przedstawione poniżej. Podobnie jak w poprzednich wydaniach badaniu poddane zostały dane zebrane z własnych narzędzi służących do administrowania ruchem do serwerów. Przeanalizowaliśmy dane za okres od 01.03.2020 do 31.03.2020. Do analizy statystycznej użyte zostały takie parametry jak dzienna liczba zdarzeń, najczęściej występujące incydenty, podział zagrożeń ze względu na rodzaj oraz potencjalną dotkliwość zdarzenia. W badanym okresie odnotowaliśmy znaczący spadek prób ingerencji w nasze systemy. Udało nam się wyodrębnić 18.305 zdarzeń w marcu. Średnia liczba zagrożeń w tym miesiącu wyniosła 590 zdarzeń dziennie. Liczbę zdarzeń występujących w każdym dniu zeszłego miesiąca obrazuje *Wykres nr 1.*

Wykres nr 1 Liczba wykrytych zdarzeń w marcu

W marcu ponownie liczba prób kompromitacji naszych serwerów utrzymywała się średnio na stałym poziomie. Naszą uwagę podczas przygotowywanie publikacji zdecydowanie przykuły dwa dni – 17.03.2020 0raz 27.03.2020. Wtedy odnotowaliśmy znaczący wzrost prób zagrożenia naszym systemom – odpowiednio 3.173 oraz 2.997. Poniżej prezentujemy tabele, w których przedstawione zostały rodzaje zagrożeń oraz liczba takich zdarzeń w danym dniu.

Rodzaj zagrożenia	*Liczba zdarzeń*
MS-RDP Brute-force Attempt	3058
UNIX Portmapper Remote Information Retrieving Attempt	64
HTTP Non RFC-Compilant Response	21
DNS RRSIG Query Type Packet	15
DNS Zone Transfer AXFR	8
PHP CGI Query String Handling Information Disclosure and DoS Vulnerability	5
HTTP OPTIONS Method	2

Tab. nr 1 Typy zdarzeń oraz ich liczba w dn. 17.03.2020 r.

Rodzaj zagrożenia	*Liczba zdarzeń*
MS-RDP Brute-force Attempt	2755
UNIX Portmapper Remote Information Retrieving Attempt	105
OpenSSH AES-GCM Auth Remote Code Execution Vulnerability	101
ZmEu Scanner Detection	19
PHP CGI Query String Parameter Handling Information Disclosure and DoS Vulnerability	9
HTTP Non RFC-Compliant Response Found	5
FTP: login Brute-force attempt	1
HTTP OPTIONS Method	1
MailEnable IMAP Server Long Tag anomaly	1

Tab. nr 2 Typy zdarzeń oraz ich liczba w dn. 17.03.2020 r.

Przedstawiamy Wam też nasz Top 20, czyli listę najbardziej popularnych zagrożeń w marcu. Są to najczęściej wykorzystywane typy zagrożeń, poprzez użycie których atakujący próbowali skompromitować naszą infrastrukturę. Poniżej tabela zagrożeń wraz z liczbą zdarzeń.

Rodzaj zagrożenia	Liczba zdarzeń
MS-RDP Brute-force Attempt	8868
HTTP SQL Injection Attempt	3286
UNIX Portmapper Remote Information Retrieving Attempt	2440
OpenSSH AES-GCM Auth Remote Code Execution Vulnerability	2034
HTTP Non RFC-Compliant Response Found	563
ZmEu Scanner Detection	369
PHP CGI Query String Parameter Handling Information Disclosure and DoS Vulnerability	175
DGA NXDOMAIN response Found	94
HTTP Directory Traversal Vulnerability	71
HTTP OPTIONS Method	65
FTP: login Brute-force attempt	53
DNS RRSIG Query Type Packet	46
Microsoft Windows win.ini access attempt	42
DNS Zone Transfer AXFR Attempt	37
DNS Zone Transfer AXFR Response	37
MailEnable IMAP Server Long Tag	29
WordPress Cuckootap Theme Arbitrary File Download Vulnerability	18
OpenSSL TLS Heartbeat Information Disclosure Vulnerability - Reverse Heartbleed	13
HTTP Unauthorized Brute-force Attack	11
WordPress MailPoet Newsletters	9

Tab. nr 3 Typy zdarzeń oraz ich liczba w marcu

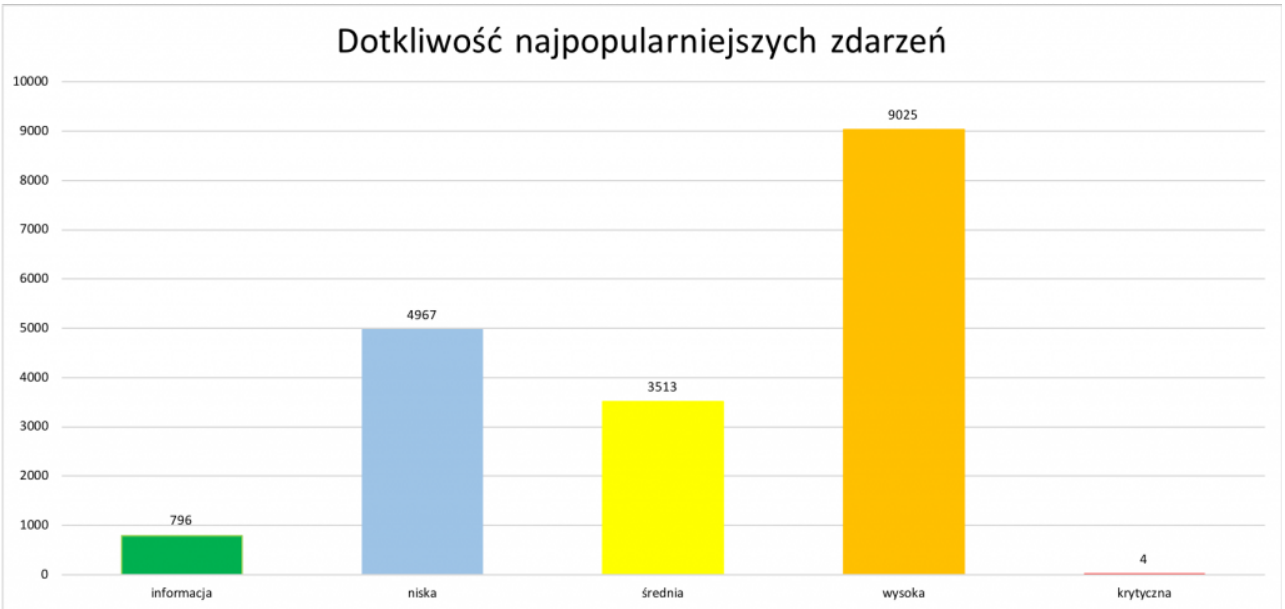
Wyżej wspominamy o pojęciu potencjalnej dotkliwości zdarzenia. Jak sama nazwa wskazuje jest to szacowany zakres szkód jakie może wyrządzić dana podatność w naszej infrastrukturze o ile dojdzie do jej pomyślnego wykorzystania. Samą dotkliwość można podzielić na 5 różnych poziomów:

- Informacja – podejrzane zdarzenie, które nie stanowi bezpośredniego zagrożenia, ale poprzez samo jego zgłoszenie uwaga administratora może zostać zwrócona na głębsze problemy infrastruktury, które mogą zaistnieć w przyszłości.
- Niska – najniższy poziom dotkliwości wymagający ostrzeżenia. Zagrożenie ma znikomy wpływ na infrastrukturę organizacji. Zazwyczaj wymagają lokalnego bądź fizycznego dostępu do systemu i często mogą powodować problemy z prywatnością ofiary lub

problemy powiązane z DoS oraz możliwy wyciek danych.

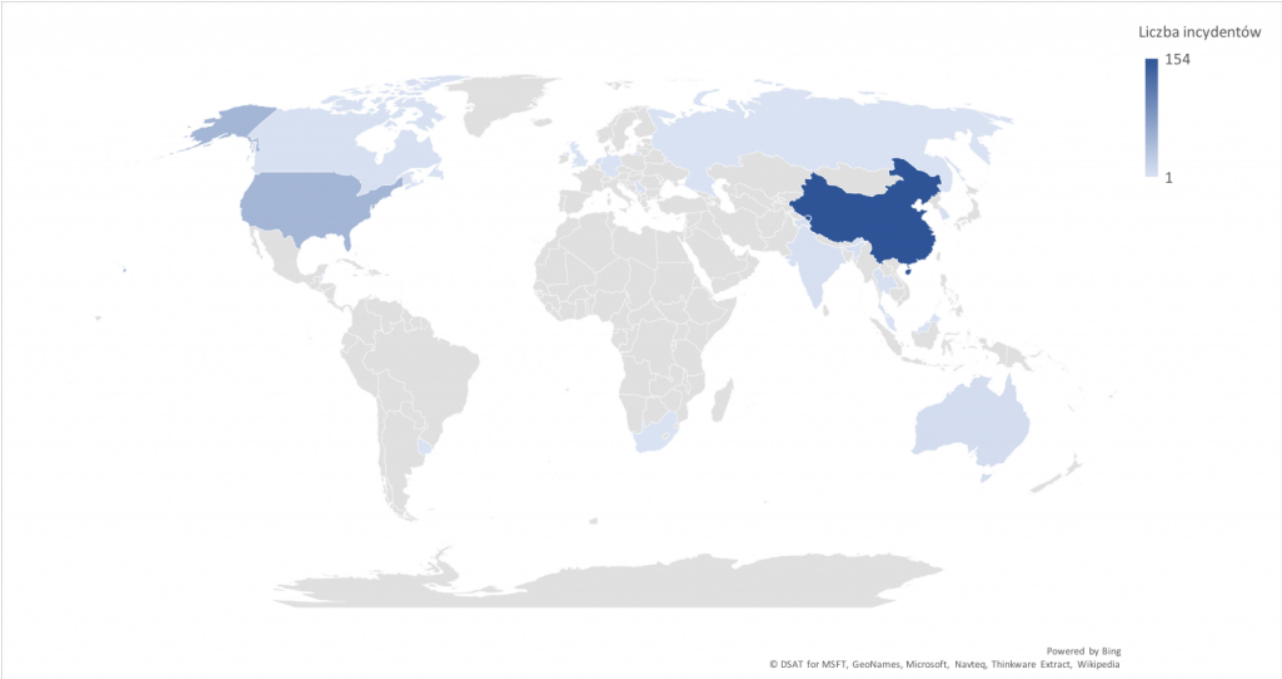
- Średnia – niewielkie zagrożenie, którego wpływ na infrastrukturę jest minimalny. Następstwem wykorzystania podatności z tej kategorii mogą być ataki typu DoS, które nie zagrażają celowi lub exploity, które od osoby atakującej wymagają przebywania w tej samej sieci LAN co ofiara. Zagrożenia poziomu średniego mogą mieć wpływ jedynie na niestandardowe konfiguracje oraz mało znane aplikacje. Zapewniają atakującemu bardzo ograniczony dostęp.
- Wysoka – zagrożenie, które potencjalnie może stać się krytycznym, jednak dzięki występowaniu czynników łagodzących nie jest możliwa jego eskalacja. Do kategorii zagrożeń poziomu wysokiego można zaliczyć zagrożenia, które są trudne do wykorzystania, nie dają podwyższonych uprawnień lub są w stanie dotknąć małej ilości ofiar.
- Krytyczna – zagrożenie poważne, które jest stanie dotknąć domyślnych instalacji szeroko rozpowszechnionego oprogramowania. Skutkuje kompromitacją serwera, a kod exploitacji jest powszechnie dostępny. Atakujący zwykle nie potrzebuje żadnych specjalnych danych uwierzytelniających ani wiedzy na temat poszczególnych ofiar, a cel nie musi być zmanipulowany w celu wykonywania jakichkolwiek specjalnych funkcji.

Na poniższym wykresie przedstawiliśmy potencjalną dotkliwość najpopularniejszych zdarzeń występujących w badanym okresie.



Wykres nr 2 Potencjalna dotkliwość najpopularniejszych zdarzeń w badanym okresie.

Podobnie jak ostatnio chcieliśmy sprawdzić z jakich krajów najczęściej pochodziły ataki. Aby to zrobić ponownie wykorzystaliśmy napisany przez nas program w bashu, który identyfikował adresy IP i przypisywał każdemu z nich kraj ich pochodzenia, a następnie je zliczał. W ten sposób otrzymaliśmy 245 unikalnych adresów IP wraz z ich krajem pochodzenia. Tym samym udało nam się zidentyfikować 18 krajów, z których próbowano skompromitować nasze usługi. Wszystkie atakujące nas państwa pokazaliśmy na poniższej mapie. Im ciemniejszy i bardziej nasycony kolor tym więcej ataków z danego miejsca odnotowaliśmy.



Mapa nr 1 Kraje próbujące atakować infrastrukturę S.M.S. w badanym okresie.

Analiza przypadku wybranych zgłoszeń

Chyba każdy marzył kiedyś chociaż przez chwilę o pracy bez konieczności wychodzenia z domu. Klepanie kodu, zamówień czy wykonywanie innych obowiązków leżąc w łóżku byłoby idealnym planem pracy. Niestety marzenia czasami spełniają się niekoniecznie w taki sposób, jak byśmy sobie tego życzyli. W związku z obecną sytuacją na świecie, pracodawcy powinni w miarę możliwości zlecić pracownikom pracę zdalną. Niesie to za sobą szereg udogodnień jak i problemów. Ponieważ lubujemy się w wyszukiwaniu i rozwiązywaniu problemów, plusy pracy zdalnej zostawimy do omówienia komuś innemu. My natomiast

w marcowej analizie skupimy się na jedynym z największych mankamentów związanych ze zdalnym dostępem, który wzbudził nasze zainteresowanie w minionym okresie.

System Windows został wyposażony we wbudowany komponent, którego nazwę większość z naszych czytelników powinna kojarzyć, a mianowicie Remote Desktop Protocol. Pozwala on na zalogowanie się do zdalnego komputera przy użyciu jego adresu IP, przez domyślny port 3389. Po pomyślnym zalogowaniu, możemy w pełni korzystać z naszej stacji roboczej, na której pracowaliśmy dotychczasowo w firmie. Jest to rozwiązanie bardzo ciekawe i pomocne, ale jednocześnie naszym zdaniem nie spełnia podstawowych standardów bezpieczeństwa systemów i sieci. Bez dodatkowego zabezpieczenia w postaci chociażby hasła, potencjalny włamywacz musi znać jedynie adres IP urządzenia, na którym uruchomiona jest usługa zdalnego pulpitu.

Jak mogliście zauważyć w ogólnej analizie statystycznej, marzec obfitował w atak o nazwie „MS-RDP Brute-force Attempt”. Jest to w ostatnim czasie utrapienie wszystkich specjalistów zajmujących się bezpieczeństwem sieci. Ale nie wybiegajmy za bardzo w przyszłość i na początek skupmy się na wprowadzeniu.

Na czym polega ten cały atak?

Alegorią ataku RDP brute-force może być włamywacz, który przed sobą ma drzwi, a w ręku pęk kluczy. Atakujący używa kluczy jeden po drugim, aby drzwi otworzyć. Im lepszy jest zamek, tym więcej czasu zajmie mu próba włamania się. Finalnie jednak prędzej czy później i tak dostanie się do środka, gdzie będzie mógł zrobić co chce.

Na tym właśnie polega omawiany atak. Hakerzy za pomocą skanerów sieciowych przeszukują Internet w celu identyfikacji zakresów portów IP i TCP, które to właśnie są używane przez serwery RDP. Po wyśledzeniu następuje właściwe działanie, podczas którego wprowadzana jest niezliczona ilość kombinacji loginu i hasła. Z ostatnio przeprowadzonych przez Microsoft badań wynika, że około 90% przypadków ataku brute-force trwa tydzień lub krócej. Co ciekawe, z tych samych badań wynika że jedynie 0,08% maszyn zostało naruszonych w wyniku ataku.

Dlaczego hakerzy przeprowadzają atak RDP?

Ransomware. Jest to główny powód, dlaczego atakujący starają się złamać nasze zabezpieczenia. Co to jest Ransomware? Jest to działanie polegające na zaszyfrowaniu plików systemowych, a następnie żądaniu od ofiary „okupu” za te właśnie pliku. Drugim, może mniej bezczelnym, ale nadal bardzo inwazyjnym celem jest keylogging. Polega on

na zainstalowaniu Keyloggera, czyli złośliwego oprogramowania, które śledzi każdy naciśnięty klawisz. Dzięki informacjom zbieranym przez programy tego typu, atakujący może gromadzić prywatne dane, takie jak np. dane karty kredytowej czy hasła.

Jak w takim razie uchronić się przez atakami typu brute-force?

Pierwszym ze sposobów ochrony jest zmiana portu RDP. Podczas skanowania sieci hakerzy najczęściej szukają połączeń korzystających z domyślnego portu RDP (3389). Biorąc ten fakt pod uwagę, zmieniając port można ukryć połączenie RDP przed skanerem.
Zmianę taką wykonuje się poprzez edycję rejestru, pod kluczem
HKEY_LOCAL_MACHINE \ System \ CurrentControlSet \ Control \ Terminal Server \ WinStations \ RDP-Tcp \ PortNumber

Niestety, działanie to nie jest niezawodną metodą ochrony i ma swoje wady. Nowoczesne skanery sprawdzają wszystkie porty dla połączeń RDP. Wypada w takim razie potraktować ten sposób ochrony jako doraźny i nie opierać się jedynie na nim.

Drugim sposobem, jaki możemy wykorzystać jest ustalenie zasad blokady konta. Jak wyżej wspomnieliśmy, działanie ataku RDP polega na wprowadzaniu niezliczonych kombinacji loginów i haseł. Można w takim przypadku ustalić, po ilu nieudanych próbach wpisania hasła konto użytkownika jest blokowane. Aby tego dokonać musimy otworzyć narzędzia administracyjne, następnie *zasady zabezpieczeń lokalnych -> zasady konta -> zasady blokowania konta* i pod rubryką „Próg blokady konta" możemy ustalić, po ilu próbach i na jak długo konto ma zostać zablokowane.

Przejdziemy teraz do ostatniego – według nas najlepszego – sposobu ochrony.

Brak odpowiedniej kontroli nad kontami uprzywilejowanymi w naszej sieci niesie za sobą ryzyko wycieku danych lub kompromitacji przedsiębiorstwa. Nadzór możliwy jest dzięki zastosowaniu przeznaczonych do tego rozwiązań z dziedziny bezpieczeństwa IT. My, do przedstawienia jak to wszystko wygląda, posłużymy się narzędziem, które całkiem niedawno zawitało w naszej firmie. Pogadajmy chwilę o systemie Fudo PAM.

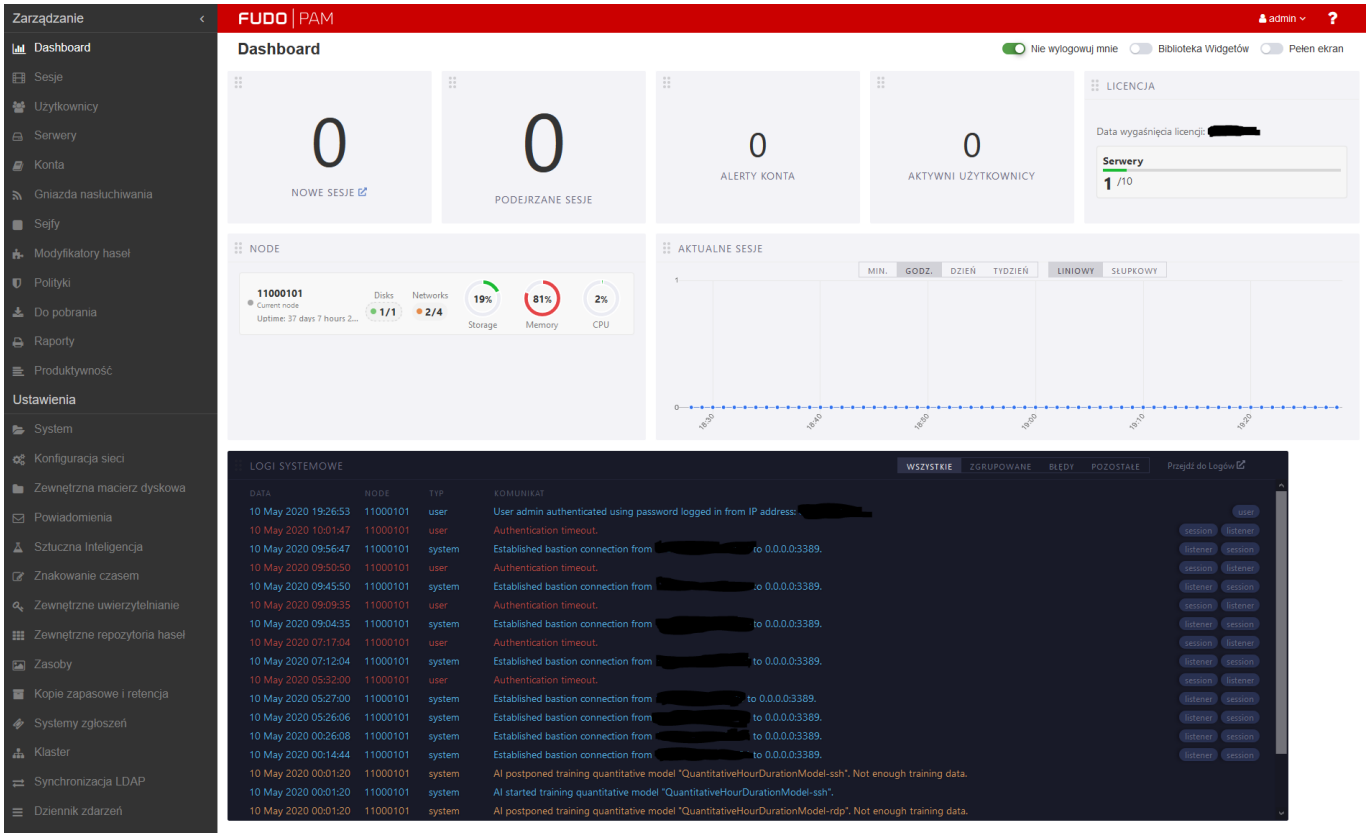
Fudo PAM jest oprogramowaniem za pomocą, którego możliwe jest zarządzanie zdalnym dostępem kont uprzywilejowanych. W tym miejscu warto również dodać, że jest to polskie rozwiązanie, z którego korzysta ponad 200 firm na całym świecie. Warto więc się chwalić, że polska myśl technologiczna odniosła sukces na arenie międzynarowej.

System składa się z czterech modułów:

- Privileged Sessions Management (PSM)
- Skarbiec haseł
- Analiza produktywności
- Application to Application Password Manager

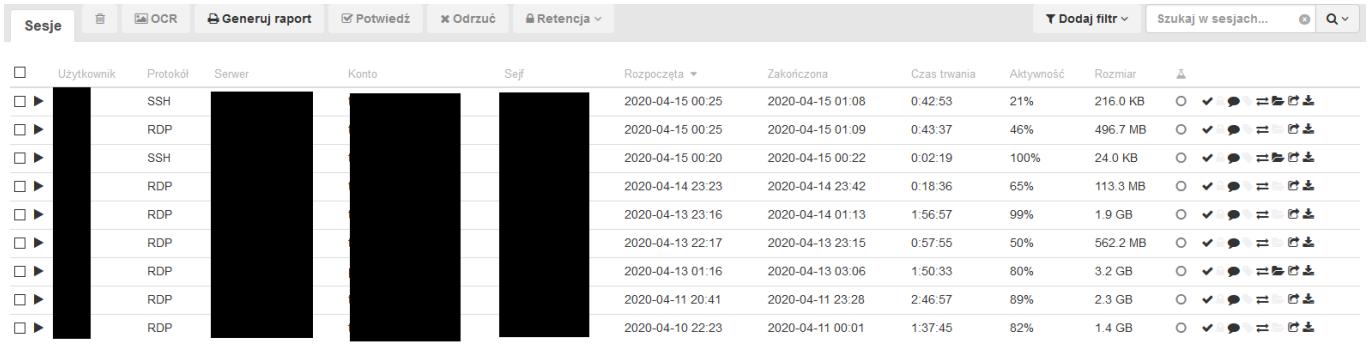
Na potrzeby tego artykułu uwagę skupimy głównie na pierwszym module.

Zarządzanie sesjami uprzywilejowanymi (Privileged Sessions Management) jest modułem służącym do stałego monitorowania zdalnych sesji. System pośredniczy w zestawieniu połączenia oraz rejestruje wszystkie akcje użytkownika. Pisząc wszystkie, mamy na myśli nawet ruch kursora myszy. Dzięki rejestrowaniu kompletnych danych możliwe jest późniejsze precyzyjne odtworzenie przebiegu sesji. Mało tego. Fudo PAM pozwala na podgląd aktualnie trwających sesji oraz ewentualną interwencję w przypadku stwierdzenia nadużycia praw dostępu.



Jakie są więc korzyści wynikające z wdrożenia systemu Fudo PAM w firmie?

Dzięki zapisowi w formacie wideo, możliwa jest szybka analiza w jaki sposób osoba nieuprawniona uzyskała dostęp do naszego systemu, co robiła oraz do jakich szkód doprowadziła. Wszystkie rejestrowane dane są zapisywane na urządzeniu Fudo w formie zaszyfrowanej, a znakowanie kryptograficznym znacznikiem czasu umożliwia późniejsze wykorzystanie nagrania jako np. dowodu sądowego.



Ogromną zaletą Fudo PAM jest intuicyjność oraz możliwość obsługi systemu poprzez przeglądarkę. Za pomocą jednego kliknięcia jesteśmy w stanie odtworzyć wybraną sesję, współdzielić ją oraz udostępnić osobom które nie posiadają konta w systemie za pomocą wygenerowanego odnośnika. Dzięki temu nie jest konieczne instalowanie dodatkowego oprogramowania

Podsumowanie

Czas pandemii postawił wszystkich administratorów sieci firmowych przed poważnym wyzwaniem. Nagła sytuacja kryzysowa wymaga dostosowania możliwości oraz organizacji pracy do obecnie panujących warunków w kraju. Ważne w tym przypadku jest nie tylko zachowanie ciągłości działania i funkcjonowania firmy poprzez przyznanie zdalnego dostępu pracownikom. Kluczowym aspektem jest skonfigurowanie go w taki sposób, aby był on odpowiednio zabezpieczony. Dlatego też wprowadzenie rozwiązań z zakresu chronionego dostępu jest jest szczególnie porządane zwłaszcza w obecnej sytuacji, kiedy ogromna część społeczeństwa pracuje z domu. Jedynie w ten sposób możemy mieć

pewność, że żadna osoba nieuprawniona nie uzyska dostępu do danych wrażliwych instytucji oraz nie doprowadzi do wycieku informacji z przedsiębiorstwa.

Poprzednie numery

Z firewall’a wzięte czyli biuletyn bezpieczeństwa komputerowego S.M.S. Nr 1 10/19

Z firewall’a wzięte czyli biuletyn bezpieczeństwa komputerowego S.M.S. Nr 2 11/19

Z firewall’a wzięte czyli biuletyn bezpieczeństwa komputerowego S.M.S. Nr 3 12/19

Z firewall’a wzięte czyli biuletyn bezpieczeństwa komputerowego S.M.S. Nr 4 01/20

Z firewall’a wzięte czyli biuletyn bezpieczeństwa komputerowego S.M.S. Nr 5 02/20

Post powstał we współpracy z Fudo Security. Nie jest to materiał sponsorowany, a wszystkie opinie zawarte w biuletynie należą do S.M.S. i są jedynie naszymi spostrzeżeniami. Serdecznie dziękujemy kolegom i koleżankom z Fudo Security za umożliwienie nam testowania rozwiązania Fudo PAM.