

CYBERWEEK, CZYLI PODSUMOWANIE TYGODNIA (01-05.03)

Czy dojdzie do eskalacji cyberkonfliktu między Indiami a Chinami, Amerykanie przegrają wyścig o prymat w dziedzinie sztucznej inteligencji z największym rywalem? I do czego tak naprawdę wykorzystywał litewską infrastrukturę rosyjski wywiad? To oraz znacznie więcej opisaliśmy w tym tygodniu na naszym portalu. Nie zabrakło również tematów związanych z social mediami i polską armią.

Polska armia skorzysta na porozumieniu z amerykańską spółką?

W poniedziałek na naszym portalu ukazał się materiał poświęcony porozumieniu zawartym między Ekspersckim Centrum Szkolenia Cyberbezpieczeństwa (ECSC) a Palo Alto Networks, którego oficjalne podpisanie miało miejsce 9 lutego br. O jego znaczeniu dla polskiej armii rozmawialiśmy z Grzegorzem Latosińskim, dyrektorem amerykańskiej spółki. Na co zwrócił szczególną uwagę?

[Co zyska polska armia na porozumieniu z Palo Alto Networks?](#)

Chiński hakerzy atakują indyjski sektor energetyczny i porty morskie

We wtorek opublikowaliśmy dwa szersze materiały dotyczące kwestii geopolitycznych. Pierwszy odnosił się do indyjsko-chińskiego cyberkonfliktu, podczas którego hakerzy chińskiej grupy sponsorowanej przez państwo przeprowadzili ukierunkowane działania w celu włamania do indyjskich organizacji. Wrogie operacje skupione były na sektorze energetycznym, a także dwóch portach morskich. Szczegółowe informacje na temat kampanii znajdują się poniżej.

[Indyjsko-chiński cyberkonflikt. Grupa RedEcho uderza w energetykę i porty morskie](#)

USA i Chiny w wyścigu o prymat w dziedzinie sztucznej inteligencji

W drugim wtorkowym materiale skupiliśmy się na amerykańsko-chińskiej rywalizacji o dominację w obszarze sztucznej inteligencji. Przedstawiliśmy stanowisko komisji USA zajmującej się AI, która jednoznacznie oceniła, że „Chiny należy uznać za konkurenta posiadającego potęgę, talent i ambicję, aby rzucić wyzwanie amerykańskiemu przywództwu technologicznemu, przewadze militarnej i silnej pozycji Stanów Zjednoczonych na świecie”. Zdaniem Kongresu Waszyngton, aby wygrać wyścig o sztuczną inteligencją z Pekinem potrzebuje „więcej pieniędzy, talentów i silniejszego przywództwa”. Jakie karty w ręku posiada Państwo Środka?

Pathfinder, czyli sposób na poprawę obrony przestrzeni powietrznej USA

Pozostajemy w temacie sztucznej inteligencji. Czas na środowy artykuł, w którym informowaliśmy o tym, że innowacyjne technologie, w tym AI, wspomogą obronę przestrzeni powietrznej Stanów Zjednoczonych. Mowa tu konkretnie o Pathfinderze, czyli rozwiązaniu przeznaczonym dla sił zbrojnych USA, które pozwala na tworzenie dokładnego obrazu operacyjnego, w celu identyfikacji ryzyka i tym samym skuteczniejszej neutralizacji zagrożenia. Pozwala ono na łączenie danych z ponad 300 źródeł wojskowych, komercyjnych i rządowych. W jaki sposób innowacyjne narzędzie odmieni operacje prowadzone przez amerykańskie wojsko?

[Sztuczna inteligencja wesprze obronę przestrzeni powietrznej USA](#)

Setki kont znika z Instagrama. W tle protesty ws. Nawalnego

W czwartek opisaliśmy kampanię usuwania 530 kont na Instagramie, które powstały głównie w Rosji i były skierowane do odbiorców krajowych podczas ostatnich protestów popierających Aleksieja Nawalnego. O wszystkim poinformował Facebook w swoim oficjalnym komunikacie, wskazując, że wspomniane konta działały na rzecz zagłuszenia komunikacji związanej z organizacją wystąpień przeciwko władzy.

[„Hashtag poisoning”: zakłócanie protestów poparcia dla Nawalnego](#)

Kto rządzi na Facebooku?

W piątek na naszym portalu pojawiły się dwa materiały, poruszające jakże ważne w obecnych czasach problemy: social mediów oraz rosyjskich cyberoperacji. W pierwszym artykule przedstawiliśmy wyniki badań przeprowadzonych przez specjalistów Cybersecurity for Democracy, które wskazują, że skrajnie prawicowe źródła wiadomości na Facebooku są bardziej angażujące od pozostałych. Całość obudowaliśmy szerszym komentarzem dotyczącym m.in. roli influencerów na portalach społecznościowych.

[Skrajna prawica rządzi na Facebooku? To nie jedyny problem mediów społecznościowych](#)

Rosyjskie cyberszpiegostwo w regionie Morza Bałtyckiego

Z kolei drugi z piątkowych materiałów odnosi się do działań Moskwy w cyberprzestrzeni w regionie Morza Bałtyckiego, w tym Polski. Litewskim służby ustaliły, że rosyjski wywiad wykorzystywał infrastrukturę na Litwie do prowadzenia ataków na cele znajdujące się w innych krajach. Wrogie działania były skierowane również wobec wysokich rangą litewskich urzędników, a także instytucji państwowych zajmujących się bezpieczeństwem, polityką zagraniczną, energetyką oraz edukacją. Poza cyberszpiegostwem Moskwa miała prowadzić także szereg innych kampanii, takich jak operacje wpływu. Jednym z głównych źródeł zagrożenia jest grupa hakerska Cozy Bear (APT29) powiązana z

rosyjskim wywiadem. Litewskie służby odniosły się także do zagrożeń płynących ze strony innych państw. Jakich?

[Rosja wykorzystała infrastrukturę Litwy do cyberszpiegostwa](#)
