Witaj w PDC News! Jesteśmy tutaj po to, żeby dostarczać Ci najważniejszych informacji ze świata cyberbezpieczeństwa. Co tydzień przygotowujemy kompleksowe zestawienie informacji, będące przewodnikiem po zagrożeniach, trendach i regulacjach z obszaru cyberbezpieczeństwa. Niezależnie od tego, czy interesuje Cię ochrona danych, ataki hakerskie czy innowacyjne rozwiązania, w PDC News znajdziesz wartościowe treści, które pomogą Ci być na bieżąco. Zapraszamy do lektury!

CYBERPOLICY

W życie weszły przepisy przyjęte w ramach ustawy o zwalczaniu nadużyć w komunikacji elektronicznej. Od 25 marca przedsiębiorcy telekomunikacyjni mają obowiązek blokować wiadomości podszywające się pod podmioty publiczne.
Więcej informacji TUTAJ.

Parlament Europejski zagłosował za tym, aby ustanowić ramy Tożsamości Cyfrowej Unii Europejskiej. Konsorcjum POTENTIAL może teraz przyspieszyć realizację projektu pilotażu Europejskiego Portfela Tożsamości Cyfrowej.
Więcej informacji TUTAJ.

Pełnomocnik Rządu ds. Cyberbezpieczeństwa Krzysztof Gawkowski wydał rekomendację dla podmiotów krajowego systemu cyberbezpieczeństwa dotyczącą bezzwłocznej aktualizacji produktów Fortinet.
Więcej informacji TUTAJ.

Rada Europejska przyjęła rozporządzenie ustanawiające nowe ramy tożsamości cyfrowej (eIDAS 2). Ma ono zapewniać obywatelom i przedsiębiorstwom w całej Europie powszechny dostęp do bezpiecznej i wiarygodnej identyfikacji elektronicznej i uwierzytelniania elektronicznego.
Więcej informacji TUTAJ.

Rada Europejska przyjęła rozporządzenie o wolności mediów. Ustanawia ono wspólne ramy dla usług medialnych na rynku wewnętrznym UE i wprowadza środki mające na celu ochronę dziennikarzy i dostawców mediów przed ingerencją polityczną.
Więcej informacji TUTAJ.

CYBER ŚWIADOMOŚĆ

Stopnie alarmowe cyberprzestrzeni są sygnałem dla służb i administracji publicznej do zachowania szczególnej czujności. W przypadku zagrożenia wystąpieniem zdarzenia o charakterze terrorystycznym, dotyczącego systemów teleinformatycznych, organów administracji publicznej lub systemów wchodzących w skład infrastruktury krytycznej albo w przypadku wystąpienia takiego zdarzenia, można wprowadzić jeden z czterech stopni alarmowych CRP.
Więcej informacji TUTAJ.

CERT Polska ostrzega przed rosnącą liczbą oszustw finansowych w internecie.
Więcej informacji TUTAJ.

Oprogramowanie Scareware: co to jest, przykłady i jak się przed nim bronić?
Więcej informacji TUTAJ.

ENISA opublikowała podsumowanie tegorocznego raportu „Foresight Cybersecurity Threats for 2030", zawierające ranking 10 najważniejszych zagrożeń dla cyberbezpieczeństwa, w perspektywie do 2030 roku.
Więcej informacji TUTAJ.

Małe i średnie firmy są w takim samym stopniu narażone na ataki hakerskie jak duże korporacje. Główne zagrożenia to ransomware oraz ataki typu Business Email Compromise (BEC).
Więcej informacji TUTAJ.

Kontakt: pdc@nask.pl