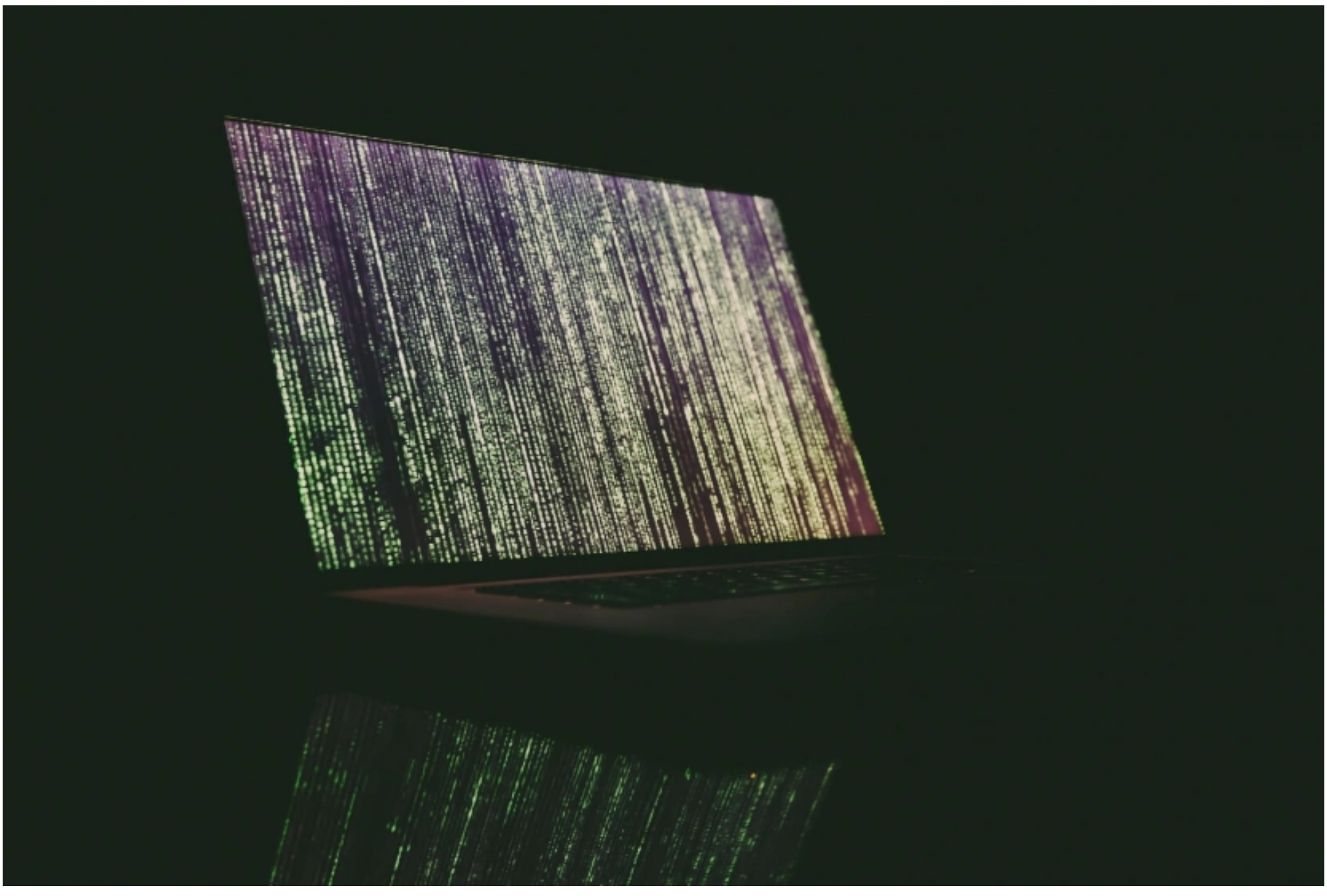
Czym jest szyfrowanie?

Michael Crider, 12.10.2021, godz. 15:56 Bezpieczeństwo kryptografia cyberbezpieczeństwo internet

Szyfrowanie zabezpiecza prywatne dane przed ciekawskimi oczami. To proste pojęcie, ale realia jego użycia są niezwykle skomplikowane.



Markus Spiske\Unsplash

Podstawy kryptografii

Na najprostszym, podstawowym poziomie, szyfrowanie jest sposobem maskowania informacji w taki sposób, aby nie można było uzyskać do nich natychmiastowego dostępu. Szyfrowanie było stosowane od tysięcy lat, na długo przed nastaniem ery informacyjnej, w celu ochrony wrażliwej lub cennej wiedzy. Wykorzystanie i badanie szyfrowania, kodów i innych środków ochrony lub ukrywania informacji nazywa się kryptografią.

Najprostszą wersją szyfrowania jest podstawowy szyfr zastępczy. Jeśli użyjesz liczb do oznaczenia liter w alfabecie łacińskim, A=1, B=2, i tak dalej, możesz wysłać wiadomość jako taki kod. Nie jest on natychmiast rozpoznawalny, ale każdy, kto zna kod, może szybko odszyfrować wiadomość. Tak więc, pozornie losowy ciąg liczb:

20 8 5 16 1 19 19 23 15 18 4 9 19 19 23 15 18 4 6 9 19 8

...może stać się istotną informacją dla kogoś, kto wie, jak go odczytać.

t he p a s s w o r d i s s w o r d f i s h

To bardzo porsty przykład, taki, jaki można znaleźć w klasycznej zabawce z pierścieniem dekodującym. Archeolodzy znaleźli przykłady ludzi szyfrujących informacje pisane, które mają tysiące lat: Mezopotamscy garncarze wysyłali sobie zakodowane wiadomości w glinie, mówiąc swoim przyjaciołom, jak zrobić nową glazurę bez informowania o tym konkurencji. Innym przykładem jest zestaw greckich substytutów zwanych kwadratem Polybusa, który wymaga klucza do odblokowania wiadomości. Używano go jeszcze w średniowieczu.

Zobacz również:

- Dostosowanie strategii bezpieczeństwa do celów ESG: Następny ważny problem dla CISO
- Rozstrzygnięto konkurs MON z tematyki cyberbezpieczeństwa
- Cyberprzestępczość 2022 - nowe trendy

Kryptografia w czasie wojny

Kryptografia jest wykorzystywana do ochrony informacji, a nie ma bardziej istotnego zastosowania niż działania wojenne. Wojsko szyfruje swoje wiadomości, aby upewnić się, że wrogowie nie poznają ich planów, jeśli komunikacja zostanie przechwycona. Analogicznie, wojsko próbuje złamać szyfrowanie, odkrywając wzór na kod bez posiadania oryginalnego klucza. Obydwie te dziedziny w znacznym stopniu przyczyniły się do rozwoju kryptografii.

Dwa doskonałe przykłady praktycznego szyfrowania znajdziemy sięgnąwszy pamięcią do II wojny światowej. Niemieckie wojsko używało fizycznego urządzenia elektronicznego zwanego maszyną Enigma, która mogła kodować i dekodować wiadomości z niewiarygodną złożonością, umożliwiając szybką i tajną komunikację. Jednak dzięki połączeniu odnajdywania zmieniających się codziennie kodów i zaawansowanej analizy, aliantom udało się złamać szyfrowanie maszyn Enigma. Zdobyli decydującą przewagę militarną, odsłuchując zaszyfrowane niemieckie wiadomości radiowe i uzyskując dostęp do ich prawdziwej treści.

Kod szyfrujący niekoniecznie musi być oparty na skomplikowanej matematyce. Amerykańskie wojsko wykorzystywało do tajnej komunikacji radiowej rdzennych Amerykanów - żołnierzy, którzy posługiwali się swoimi ojczystymi językami, takimi jak plemion Komanczów i Navajo. Mówiąc do siebie w tych językach, zarówno w mowie potocznej, jak i w podstawowych szyfrach słowno-literowych, szyfranci mogli przekazywać rozkazy i inne informacje drogą radiową. Wojska niemieckie, włoskie i japońskie mogły z łatwością przechwycić te transmisje, ale nie mając dostępu do żadnych rdzennych Amerykanów, ta stosunkowo prosta metoda szyfrowania była nie do złamania.

Także podczas wojny sześciodniowej w 1967 Arabowie nie mogli złamać izraelskiego szyfru, którym był… język polski [dodatek od tłum.].

Współczesne szyfrowanie elektroniczne

We współczesnym świecie szyfrowanie odbywa się prawie wyłącznie za pomocą komputerów. Zamiast szyfrować każde słowo lub literę z inną, lub nawet według jakiegoś wzoru, szyfrowanie elektroniczne szyfruje poszczególne bity danych w sposób losowy i szyfruje również klucz. Ręczne odszyfrowanie choćby niewielkiego fragmentu tych informacji, nawet przy posiadaniu właściwego klucza, zajęłoby więcej niż całe życie.

Dzięki szybkim obliczeniom dostępnym w świecie elektronicznym, dane zaszyfrowane cyfrowo są mniej lub bardziej niemożliwe do złamania konwencjonalnymi metodami. Na przykład jedynki i zera (bity), które składają się na cyfrową zawartość pliku zakodowanego przy użyciu powszechnie stosowanego 128-bitowego standardu Advanced Encryption Standard, są zakodowane dziesięć razy w półlosowy sposób. Innemu komputerowi, bez klucza, ponowne ułożenie ich w prawidłowej kolejności zajęłoby tyle czasu, że słońce wypaliłoby się, zanim zostałoby złamane. I to jest właśnie najsłabsza wersja AES: występuje również w wersjach z kluczem 192- i 256-bitowym!

Do czego przydaje się szyfrowanie?

Każdy duży współczesny system operacyjny zawiera przynajmniej kilka narzędzi do szyfrowania danych: Windows, macOS, iOS, Android i Linux. System Bitlocker w systemie Windows jest jednym z przykładów. W mniejszym lub większym stopniu możesz zaszyfrować wszystkie swoje dane tak, aby do ich odblokowania potrzebny był klucz. To samo dotyczy przechowywania plików online oraz danych osobowych przechowywanych w innych bezpiecznych miejscach, np. w banku.

Aby uzyskać dostęp do zaszyfrowanych informacji, można użyć jednego z trzech różnych typów kluczy. W zabezpieczeniach komputerowych są one określane jako coś, co się wie (hasło lub kod PIN), coś, co się posiada (fizyczny klucz szyfrujący, taki jak Yubico) i coś, czym się jest (uwierzytelnianie biometryczne, takie jak odcisk palca lub skan twarzy).

Szyfrowanie pamięci masowej urządzeń chroni je w sensie czysto elektronicznym: bez jednej z tych metod odblokowania dostęp do danych jest niezwykle trudny - wręcz niemożliwy. Dodatkowe przetwarzanie, które jest potrzebne do zaszyfrowania i odszyfrowania danych, może sprawić, że pamięć masowa komputera będzie działać wolniej, ale nowoczesne oprogramowanie może pomóc zminimalizować ten spadek prędkości.

Oczywiście, jeśli ktoś inny ma dostęp do naszego hasła, klucza fizycznego lub odcisku palca, może uzyskać dostęp do tych danych. Dlatego dobrze jest stosować dodatkowe metody bezpieczeństwa. Popularny system uwierzytelniania dwuskładnikowego (2FA) wykorzystuje do logowania zarówno hasło (coś, co znasz), jak i wiadomość tekstową wysyłaną na Twój telefon (coś, co posiadasz). Daje to dodatkową warstwę

bezpieczeństwa dla wszelkich informacji przechowywanych w tym systemie. Korzystanie z menedżera haseł do tworzenia unikalnych haseł dla każdej witryny lub usługi, z której korzystasz, zapewnia jeszcze większą ochronę, uniemożliwiając hakerom ponowne wykorzystanie Twoich danych logowania, jeśli uda im się przechwycić nasze dane uwierzytelniające do danej usługi.

Szyfrowanie danych nie oznacza, że jest absolutnie niemożliwe, aby uzyskać do nich niewłaściwy dostęp. Zawsze istnieją słabe punkty i sposoby na obejście zabezpieczeń. Ale stosowanie nawet podstawowych narzędzi szyfrowania może pomóc chronić dane w stopniu znacznie przekraczającym to, co jest dostępne domyślnie.

Tłum. i oprac. Anna Ładan

Źródło

Urządzenia IoT zagrażają w coraz większym stopniu korporacyjnym systemom IT

Janusz Chustecki, 14.12.2021, godz. 12:26 Bezpieczeństwo Sieci IoT Microsoft

Grafika: jeferrb/Pixabay

Botnety IoT powodują coraz więcej problemów związanych z tym, że zaczynają atakować swoje zaplecze, czyli centra danych. Dlatego Microsoft przeprowadził ostatnio badanie, mające pokazać, czy urządzenia instalowane na obrzeżach sieci zagrażają rzeczywiście korporacyjnym systemom IT.

Ankieta przeprowadzona na zlecenie Microsoftu przez Instytut Ponemon dotyczyła urządzeń Internetu Rzeczy (IoT) i operacji OT (Operational Technology) oraz zagrożeń, jakie stwarzają one dla systemów IT, które kiedyś były odseparowane od urządzeń sieci brzegowych, a obecnie są z nimi ściśle integrowane.

Ankieta przeprowadzona wśród informatyków zajmujących się bezpieczeństwem IT wykazała, że połowa urządzeń OT jest podłączona do korporacyjnych sieci IT. Około 88% respondentów stwierdziło, że ich biznesowe urządzenia IoT są połączone z internetem (np. z usługami drukowania w chmurze), podczas gdy 56% stwierdziło, że urządzenia OT wspierają wtedy zdalny dostęp.

Microsoft wskazuje tu na botnet Mozi P2P IoT, którego celem jest wprowadzanie szkodliwego oprogramowania do rejestratorów wideo i do innych produktów IoT, w tym do sieciowych bram. Mozi pokazuje, w jaki sposób sieci biznesowe mogą zostać naruszone przez zhakowane urządzenia brzegowe, które kiedyś uważano za całkowicie nieszkodliwe.

Ankieta Ponemon Institute wykazała, że tylko 29% respondentów posiada pełną inwentaryzację urządzeń IoT i OT. Większość respondentów (64%) nie wie, czy ich urządzenia IoT są załatane. Tyle samo przyznaje, że nie wie czy do ich urządzeń ktoś się kiedykolwiek włamał.

Wiele ataków na urządzenia VPN w ciągu ostatniego roku pokazało również, że może to być słaby punkt w sieciach korporacyjnych i przemysłowych. Badanie sugeruje, że menedżerowie IT są świadomi takich zagrożeń, ponieważ 39% z nich stwierdziło, że doświadczyło ataku na urządzenia IoT lub OT w ciągu ostatnich dwóch lat.

Ponadto 35% stwierdziło, że doświadczyło incydentu, w którym urządzenie IoT zostało użyte do przeprowadzenia szerszego ataku, takiego jak oprogramowanie ransomware, lub w celu uzyskania trwałości w sieci. Większość respondentów (63%) uważa też, że skala ataków na urządzenia IoT/OT znacznie wzrośnie w nadchodzących latach.

Nowe wydanie Computerworld

Wanda Żółcińska, 15.12.2021, godz. 12:01 Computerworld Bezpieczeństwo sztuczna inteligencja Biznes i zarządzanie

Już jest najnowsze, grudniowe wydanie Computerworld. W jakim charakterze warto zatrudnić sztuczną inteligencję i w jaki sposób współpracować w organizacji w trybie hybrydowym?

W najnowszym wydaniu Computerworld jak zwykle wiele uwagi poświęcamy zarządzaniu, budowaniu przewag konkurencyjnych dzięki technologii. Jednym z czynników, które pozwalają na przyspieszenie rozwoju firmy jest wykorzystanie sztucznej inteligencji. Jakie wyzwania się z tym wiążą?

Piszemy także o najlepszych praktykach w obszarze pracy hybrydowej, która już na stałe wpisała się w krajobraz działania firm.

Cyberbezpieczeństwo zawsze jest w centrum naszej uwagi. W najnowszym wydaniu piszemy m.in. o XDR, który wyznacza kierunek rozwoju systemów bezpieczeństwa.

W dziale poświęconym technologii koncentrujemy się na odpowiedzi na pytanie, czy najnowszy standard Wi-Fi, czyli Wi-Fi 6, zapewnia większą przepustowość i szybkość komunikacji? Piszemy także o zaletach modelu multicloud, który zyskuje coraz większą popularność.

Zapraszamy do lektury!

Znajdź nas