Chroń swoją firmę przed atakami z użyciem oprogramowania ransomware

Według raportu Official Annual Cybercrime Report (Oficjalny doroczny raport na temat cyberprzestępczości) co 14 sekund kolejna firma pada ofiarą ataku przeprowadzonego przy użyciu oprogramowania ransomware. Ryzyko jest jeszcze wyższe teraz, gdy pracownicy pracują z domu poza firmowym firewallem.

Co to jest?

Ransomware to złośliwe oprogramowanie blokujące dostęp do systemu komputerowego lub urządzenia, dopóki użytkownik nie zapłaci „okupu". To złośliwe oprogramowanie wyszukuje i szyfruje ważne dane oraz uniemożliwia użytkownikowi dostęp do systemu operacyjnego, żądając dokonania opłaty, zazwyczaj w bitcoinach lub innej kryptowalucie, za ujawnienie klucza odszyfrowującego.

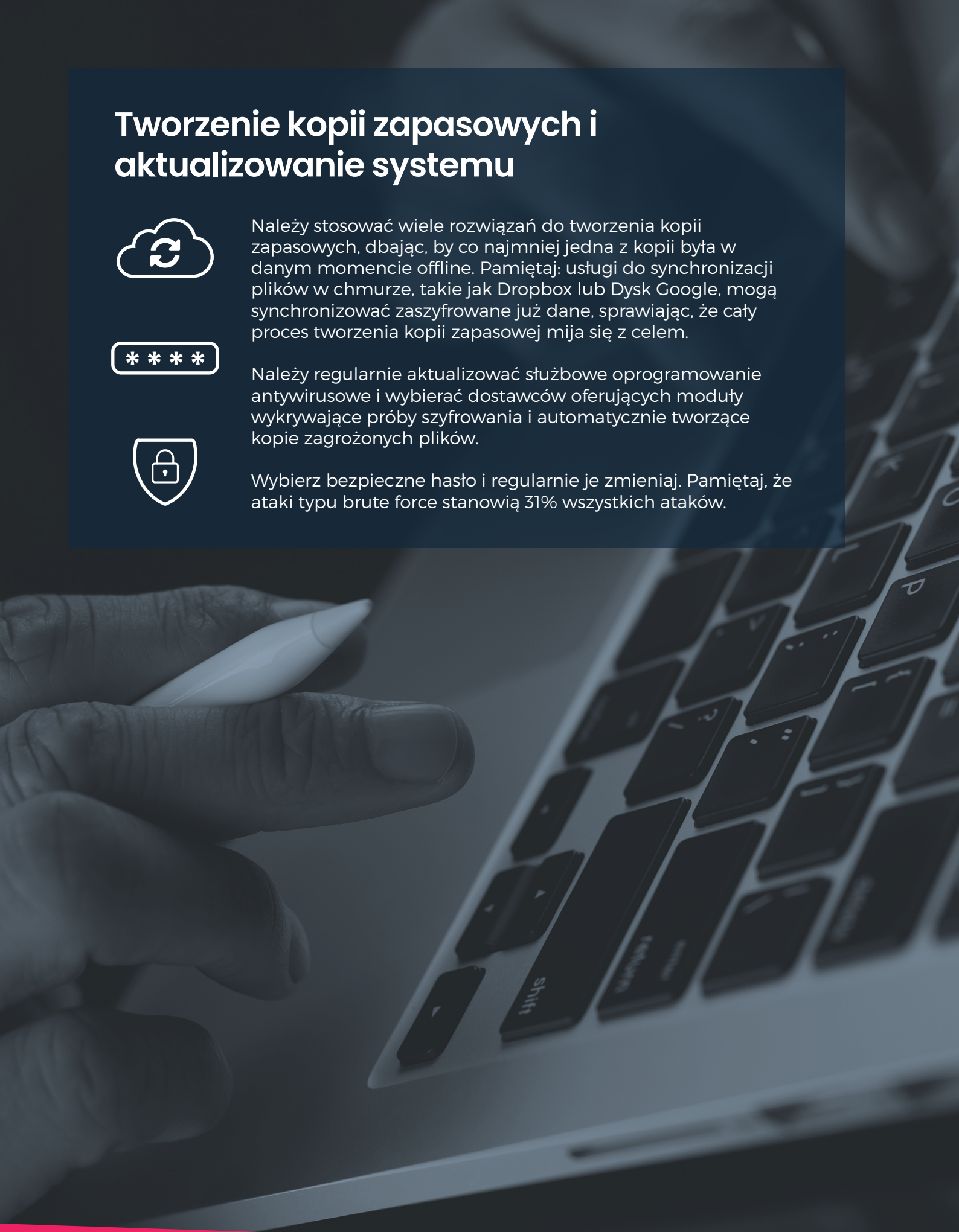
Nie ma gwarancji, że zapłata okupu spowoduje odzyskanie przez ofiarę dostępu do swojego urządzenia i danych.

Tworzenie kopii zapasowych i aktualizowanie systemu

Należy stosować wiele rozwiązań do tworzenia kopii zapasowych, dbając, by co najmniej jedna z kopii była w danym momencie offline. Pamiętaj: usługi do synchronizacji plików w chmurze, takie jak Dropbox lub Dysk Google, mogą synchronizować zaszyfrowane już dane, sprawiając, że cały proces tworzenia kopii zapasowej mija się z celem.

Należy regularnie aktualizować służbowe oprogramowanie antywirusowe i wybierać dostawców oferujących moduły wykrywające próby szyfrowania i automatycznie tworzące kopie zagrożonych plików.

Wybierz bezpieczne hasło i regularnie je zmieniaj. Pamiętaj, że ataki typu brute force stanowią 31% wszystkich ataków.



Czynnik ludzki

Należy szkolić pracowników, aby rozpoznawali i zgłaszali podejrzane e-maile – oprogramowanie ransomware łatwo rozprzestrzenia się za pośrednictwem spamu i e-maili phishingowych.

Korzystaj z rozwiązań z zakresu skanowania treści i filtrów e-mailowych, aby zapewnić sobie dodatkową warstwę zabezpieczeń. Te narzędzia potrafią wykrywać szkodliwe linki i usuwać niebezpieczne e-maile, zanim trafią do pracowników.

Upewnij się, że w firmie obowiązuje znormalizowana procedura bezpieczeństwa, która obowiązuje wszystkich, począwszy od pracowników po członków zarządu.

Opracuj plan postępowania w sytuacji kryzysowej obejmujący podjęcie odpowiednich kroków w odpowiedzi na potencjalny atak. Uwzględnij zarówno ramy techniczne, jak i strategie w celu złagodzenia konsekwencji prawnych i uszczerbku na reputacji.

Sprawdź u swojego ubezpieczyciela, czy Twoja polisa obejmuje koszt związany z atakiem z użyciem oprogramowania ransomware.

Na wypadek ataku opracuj strategię PR w celu wyjaśnienia zajścia klientom, inwestorom i prasie.

Aby poznać inne specjalistyczne porady na temat cyberbezpieczeństwa dla swojego inteligentnego zakładu, przejdź na stronę www.euautomation.com