Akademia Bezpieczeństwa mBanku

odpowiedzi na pytania zadane podczas szkolenia z cyberbezpieczeństwa dla firm

mBank securitum

Udzielone przez nas odpowiedzi na pytania mają charakter ogólny i informacyjny. Firma powinna konsultować konkretne rozwiązania dotyczące bezpieczeństwa i zabezpieczeń w kontekście swojej działalności oraz infrastruktury z odpowiednimi specjalistami. Nie ponosimy odpowiedzialności za jakiekolwiek decyzje podjęte na podstawie udzielonych przez nas informacji.

1. Jak mogę sprawdzić wiarygodność faktury otrzymanej na e-maila?

W pierwszej kolejności warto sprawdzić, czy numer konta wskazany na fakturze znajduje się na tzw. “białej liście podatników VAT”, czyli rejestrze prowadzonym przez Krajową Administrację Skarbową. W ten sposób potwierdzisz numer rachunku bankowego, na który możesz zapłacić swojemu kontrahentowi.

Jeśli faktura jest nadesłana elektronicznie (mailem, przez komunikator) i zawiera inny numer rachunku niż zazwyczaj lub to pierwsza faktura od kontrahenta, potwierdź telefonicznie z kontrahentem poprawność numeru konta.

2. Gdzie można zgłaszać próby oszustw, np. próby zainfekowana urządzeń lub wyłudzenia danych?

Wszelkie próby oszustw zgłoś do CERT NASK Zgłoś incydent | CERT.PL>_

3. Jakie są najważniejsze punkty, o których trzeba pamiętać, jeżeli nasz komputer się zainfekuje?

Należy działać z procedurami ustalonymi przez daną firmę. Warto podejrzenie o infekcji jak najszybciej zgłosić do działu IT lub bezpieczeństwa. Nie należy nic instalować na własną rękę (np. dodatkowego programu antywirusowego).

4. Co zrobić jeśli adres e-mail znalazł się na serwisach wyciekowych? Czy zmiana hasła wystarczy?

Zależy to od zakresu danych, który wyciekł. Warto zmienić hasło na silne do poczty e-mail oraz skonfigurować 2FA (dwuczynnikowe uwierzytelnienie) na najbardziej istotnych kontach (np. skrzynka pocztowa).

5. Czy bezpiecznie jest zapisywać hasła w przeglądarce internetowej? Nawet jeśli generuję silne hasła do każdego portalu?

Nie rekomendujemy tego sposobu przechowywania haseł. Warto pamiętać, że jeśli na komputerze znajdzie się złośliwe oprogramowanie, to będzie w stanie takie hasła pobrać. Zamiast zapisywać hasła w przeglądarce proponujemy używać menedżera haseł. Menedżer haseł powinien być jednak odpowiednio zabezpieczony (silne hasło, 2FA, kopia zapasowa).

6. Czy menedżer haseł nie jest narażony na atak i wyciek?

Nie ma aplikacji w 100% odpornej na atak. Dlatego warto mieć skonfigurowane odpowiednio silne hasło zabezpieczające dostęp do menedżera haseł. Warto również robić kopie zapasowe menedżera haseł oraz zabezpieczyć dostęp do menedżera haseł za pomocą 2FA (dwuczynnikowego logowania).

7. Czy wszystkie aplikacje w sklepie Google Play są sprawdzone i bezpieczne?

W Google Play najczęściej znajdują się sprawdzone aplikacje, chociaż istnieje niewielkie prawdopodobieństwo umieszczenia w tym sklepie aplikacji podszywającej się pod aplikację bankową (lub inną). Aplikacje bankowe najlepiej ściągać z linków umieszczonych na stronach banku: https://www.mbank.pl/msp-korporacje/ (dolna część strony).

8. Czy jeśli kliknę w niebezpieczny link lub pobiorę zainfekowany załącznik na telefonie, na którym korzystam z poczty służbowej, mogę w ten sposób zainfekować całą swoją skrzynkę pocztową oraz skrzynki innych pracowników?

Prawdopodobieństwo automatycznego zainfekowania wszystkich użytkowników używających tego samego systemu pocztowego jest bardzo małe. Prawdopodobieństwo infekcji skrzynki danego użytkownika zależy od wykonanych przez niego akcji (np. podatnie loginu/hasła do poczty w podejrzanej aplikacji, zatwierdzenie szerokich uprawnień podejrzanej aplikacji, itd). Samo kliknięcie linku na telefonie, najczęściej nie powoduje automatycznej infekcji telefonu / skrzynki pocztowej.

9. Czy pliki PDF w e-mailu mogą być zainfekowane?

Z bardzo małym prawdopodobieństwem tak. Zazwyczaj jednak tego typu pliki używane są w zaawansowanych/złożonych atakach celowanych na pojedynczych użytkowników. Warto też posiadać zaktualizowane czytniki plików PDF – zmniejsza to jeszcze bardziej ryzyko skutecznego ataku.

10. Na co zwrócić uwagę przy instalowaniu aplikacji na telefonie?

Przy instalacji aplikacji warto zwracać uwagę, czy nie są one dystrybuowane z podejrzanego źródła (np. SMS, polecenie przez „konsultanta", link przesłany wiadomością e-mail). Należy używać aplikacji dostępnych w oficjalnych sklepach producentów (Google Play, App Store). Należy sprawdzać, czy aplikacja nie prosi o przyznanie nieznanych użytkownikowi/nadmiarowych uprawnień. Należy też minimalizować liczbę aplikacji zainstalowanych na telefonie. Miejsce, w którym możemy sprawdzić uprawnienia nadane aplikacjom może różnić się w zależności od systemu operacyjnego telefonu. W przypadku iOS można je sprawdzić w następującym miejscu: Ustawienia -> prywatność i ochrona. W przypadku systemów Android: Ustawienia -> Bezpieczeństwo i Prywatność -> Prywatność -> Menadżer uprawnień (możliwe są różnice pomiędzy telefonami opartymi o system Android).

11. Jak zareagować, jeżeli zorientujemy się, że kliknęliśmy w podejrzany link na komputerze? Jakie powinny być pierwsze kroki?

Najczęściej samo kliknięcie linku nie wyrządza szkód (dopiero zainstalowanie / otwarcie aplikacji z takiego linku bądź podanie w takim linku wrażliwych danych). Tego typu działanie zawsze warto zgłosić zgodnie z procedurami obowiązującymi w danej firmie (np. zgłosić taki fakt do działu IT lub działu bezpieczeństwa). Jednym ze sposobów ograniczenia szkód po kliknięciu takiego linku wyłączenie dostępu do internetu, a następnie zgłoszenie tego faktu do działu IT.