ZASADA CZYSTEGO EKRANU
WZROKOWA KRADZIEŻ DANYCH
SNOOPING – PODGLĄDANIE DANYCH NA EKRANIE

W CELU ZMINIMALIZOWANIA RYZYKA UTRATY DANYCH Z EKRANU MONITORA NALEŻY UŚWIADOMIĆ PRACOWNIKÓW, ŻE OKOŁO 75% DANYCH WYCIEKA PRZEZ WZROKOWĄ KRADZIEŻ DANYCH ORAZ ZDJĘCIA WYKONANE URZĄDZENIAMI ELEKTRONICZNYMI

W czasie audytów bezpieczeństwa informacji sprawdzamy **zasadę czystego ekranu**. Pracownicy często nie zdają sobie sprawy, jak ważna jest ta zasada. Nie przestrzeganie jej grozi **wyciekiem danych wrażliwych** przez podglądanie danych na ekranie. Dodatkowo, klient w sposób niezauważony, może wykonać zdjęcie z ekranu komputera, na którym są dane innego klienta lub poufne dane wrażliwe.

W czasie jednego z audytów, na prośbę audytora, została wykonano prezentację dla zarządu - wystarczyło podejść do stanowiska kasowego na odległość około 2-3 metrów, aby móc odczytać dokładnie zapisy na ekranie monitora. Prezentacja odbywała się na realnym przykładzie: przy kasie stała klientka, a za jej plecami stali audytorzy z przedstawicielem zarządu Banku i **wszyscy mogli bez żadnych ograniczeń odczytać treść z monitora**. Dane na monitorze dotyczyły **danych finansowych klientki, jej danych osobowych i zasobów finansowych zgromadzonych w banku**.

Reakcja była natychmiastowa. Na stanowisku pracy nastąpiło przeorganizowanie miejsca i monitor został ustawiony pod odpowiednim kątem co skutecznie uniemożliwiło dalsze podglądanie treści z monitora. Przeprowadzono również krótkie szkolenie uświadamiające dla całej grupy kasjerów w tym banku.

Kiedy możemy utracić dane z ekranu monitora i na co zwracać uwagę?

- W placówkach banków panuje trend otwarcia się na klienta. Często zlecenie na zaprojektowanie nowego stanowiska bezpośredniej obsługi klienta otrzymują projektanci, którzy realizują swoją wizję architektoniczną, ale niestety **nie kierują się kategoriami bezpieczeństwa fizycznego**. Należy zwrócić szczególną uwagę, aby monitor w stosunku do pracownika był ustawiony tak, by pracownik miał przez 8 godzin pracy pełny komfort i nie musiał ustawiać monitora pod kątem, żeby lepiej widzieć treści na ekranie. W ten sposób odsłaniamy monitor również dla klienta i **klient może odczytywać treści na ekranie monitora praktycznie bez ograniczeń**.

Servus Comp Sp. z o.o. Sp. K.
30-019 Kraków ul. Mazowiecka 25/502
tel. 12 631-91-22 biuro@servus-comp.pl
www.premiumbank.zadbajobezpieczenstwo.pl

- W czasie obsługi klienta, gdy musimy opuścić stanowisko aby np. wykonać kopię dokumentów dostarczonych przez klienta, lub w celu uzyskania niezbędnych informacji od współpracowników. W tym czasie klient zostaje przy opuszczonym stanowisku i ma możliwość ingerencji w treść monitora. Bezwzględnie należy pamiętać, że przed opuszczeniem stanowiska, zostawiając przy stanowisku klienta, MUSIMY BEZWZGLĘDNIE ZABLOKOWAĆ EKRAN MONITORA. W przeciwnym przypadku dajemy możliwość ingerencji wzrokowej klientowi w treść wyświetloną na ekranie, a poza tym, klient w sposób niezauważony może wykonać zdjęcie z ekranu i np. umieścić je w mediach społecznościowych, ujawniając jego pochodzenie.
  Wizerunkowo traci bank, a dodatkowo konsekwencje ponosi pracownik, który do tego dopuścił.

JAK CHRONIC TREŚĆ WYŚWIETLANĄ NA MONITORZE PRZED OKIEM WŚCIBSKIEGO KLIENTA?

- Szkolenia uświadamiające pracowników
  Nieświadomość pracowników jest sprzymierzeńcem złodziei trudniących się pozyskiwaniem danych przez podglądanie treści na monitorze.
  Wg KPMG aż:
  - **47% personelu zarządzającego w bankach** nie ma świadomości o zagrożeniu tego typu.
  - **72 % managerów niższego szczebla w ogóle tego tematu nie porusza** ze swoimi pracownikami.

  Statystykę tę potwierdzają nasze wnioski z audytów bezpieczeństwa informacji, gdyż na stanowisku pracy musimy wyjaśniać pracownikom i ich przełożonym, jak ważna jest zasada czystego ekranu i zabezpieczenie przed utratą danych.

- Stosowanie dwóch magicznych klawiszy w celu szybkiego wygaszenia monitora
  Naciśnij klawisz logo Windows + L, aby szybko zablokować ekran

servus comp
Servus Comp Sp. z o.o. Sp. K.
30-019 Kraków ul. Mazowiecka 25/502
tel. 12 631-91-22 biuro@servus-comp.pl
www.premiumbank.zadbajobezpieczenstwo.pl

Pamiętajmy, by zawsze ZABLOKOWAĆ EKRAN MONITORA przed:

- odejściem od stanowiska pracy do kserokopiarki, drukarki, do przełożonego
- wyjściem na lunch
- wyjściem do toalety
- INNE opuszczenie stanowiska pracy

BLOKOWANIE EKRANU KOMPUTERA POWINNO STAĆ SIĘ NAWYKIEM !!!

- Stosowanie automatycznych wygaszaczy ekranu ustawianych przez działy informatyki
  W środowiskach sieciowych stosowana jest polityka wygaszania ekranu w sposób automatyczny po dłuższym bezruchu komputera. Z reguły w bankach obowiązuje zasada automatycznego wygaszania ekranu po 5 – 10 lub 15 minutach bezruchu komputera. Czasami jednak kasjerzy, którzy mają zajęte ręce licząc pieniądze nie mogą wzbudzić ekranu, który wygasza się już po 5 minutach. Warto zatem przemyśleć zasady wygaszania ekranu na poszczególnych stanowiskach, tak, aby nie utrudniało to pracy.
- Stosowanie barier architektonicznych
- Stosowanie filtrów prywatyzujących

Filtry prywatyzujące są tak zaprojektowane, aby były przezroczyste, gdy patrzymy na nie na wprost, a czarne i matowe, gdy patrzymy na nie pod kątem. Filtr prywatyzujący nałożony na monitor ekranu skutecznie uniemożliwia ingerencję w treść wyświetloną na monitorze.

Filtry prywatyzujące mają szczególnie zastosowanie w bankach, gdy musimy zabezpieczyć się przed wszelkimi konsekwencjami prawnymi wynikającymi z wycieku danych wrażliwych klientów.

Filtr można nakładać bezpośrednio na ekran monitora na różne sposoby. Niektóre przylegają do ekranu jak magnes, niektóre mają części, które można zatrzasnąć bezpośrednio na górnej lub bocznej części ekranu monitora, a niektóre wyposażone są w zestawy instalacyjne, dzięki czemu filtr można zamontować na stałe.

Servus Comp Sp. z o.o. Sp. K.
30-019 Kraków ul. Mazowiecka 25/502
tel. 12 631-91-22 biuro@servus-comp.pl
www.premiumbank.zadbajobezpieczenstwo.pl

- Nakładki ograniczające widoczność na monitorze

W celu uzyskania pełnej informacji w omawianych zakresach zapraszamy do kontaktu:

Andrzej Popiołek
Audytor Wiodący SZBI, Członek IIA Polska
+48 602 220 749 andrzej.popiolek@servus-comp.pl

Ewa Niesiołowska
Audytor Wiodący SZBI, Członek IIA Polska
+48 531 364 287 ewa.niesiolowska@servus-comp.pl

Anna Stręk
Audytor Wiodący SZBI, Członek IIA Polska
+48 781 555 025 anna.strek@servus-comp.pl

Anna Kramarczyk
Kierownik ds. projektów IT
+48 794 671 787 anna.kramarczyk@servus-comp.pl

Servus Comp Sp. z o.o. Sp.k.
ul. Mazowiecka 25/502, 30-019 Kraków
Sąd Rejonowy dla Krakowa – Śródmieście,
XI Wydział Gospodarczy Krajowego Rejestru Sądowego
NIP: 6772394344 | Regon: 362815411 | KRS: 0000582481
https://zadbajobezpieczenstwo.pl
https://premiumbank.zadbajobezpieczenstwo.pl

Nota prawna:

1. Zaprezentowany materiał jest autorskim opracowaniem i jest objęty prawem autorskim.
2. Niniejszy materiał, ani żaden jego fragment nie może być reprodukowany, przetwarzany i rozpowszechniany w jakikolwiek sposób za pomocą urządzeń elektronicznych, mechanicznych, kopiujących, nagrywających i in. do celów innych niż realizacja przedmiotowej umowy u Klienta.

Servus Comp Sp. z o.o. Sp. K.
30-019 Kraków ul. Mazowiecka 25/502
tel. 12 631-91-22 biuro@servus-comp.pl
www.premiumbank.zadbajobezpieczenstwo.pl