WAMA SMART LAB

EKONOMIA WODY

WARMIŃSKO-MAZURSKIE

Fundusze Europejskie Program Regionalny

Rzeczpospolita Polska

WARMIA MAZURY Zdrowe życie, czysty zysk

Unia Europejska Europejski Fundusz Społeczny

WAMA SMART LAB
EKONOMIA WODY
WARMIŃSKO-MAZURSKIE

Cyberbezpieczeństwo w małych i średnich przedsiębiorstwach – *przegląd zagrożeń.*

mł. insp. dr inż. Michał Bukowski

Dyrektor Instytutu Służby Kryminalnej

Wydziału Bezpieczeństwa i Nauk Prawnych

Akademii Policji w Szczytnie

Fundusze Europejskie Program Regionalny

Rzeczpospolita Polska

WARMIA MAZURY Zdrowe życie, czysty zysk

Unia Europejska Europejski Fundusz Społeczny

WAMA SMART LAB

EKONOMIA WODY

WARMIŃSKO-MAZURSKIE

Wstęp

Cyberbezpieczeństwo jest niezwykle istotnym aspektem w dzisiejszym świecie biznesu, niezależnie od rozmiaru przedsiębiorstwa. Małe i średnie przedsiębiorstwa (MŚP) są często bardziej podatne na różnego rodzaju zagrożenia cybernetyczne, ponieważ często brakuje im odpowiednich zasobów i środków finansowych, by zainwestować w zaawansowane rozwiązania. Oto przegląd głównych zagrożeń, które MŚP mogą spotkać w obszarze cyberbezpieczeństwa:

WAMA SMART LAB
EKONOMIA WODY
WARMIŃSKO-MAZURSKIE

Główne zagrożenia:

Ataki phishingowe

Malware

Braki w aktualizacjach

Słabe hasła

Nieaktualne oprogramowanie antywirusowe i antymalware

Brak szkoleń dla pracowników

Ataki DDoS

Nieautoryzowany dostęp

Zagrożenia związane z dostawcami

Zagrożenia związane z mobilnością

Cyberprzestępczość ukierunkowana na MŚP

Brak strategii zarządzania incydentami

WAMA SMART LAB
EKONOMIA WODY
WARMIŃSKO-MAZURSKIE

Ataki phishingowe

Nazwa phishing budzi dźwiękowe skojarzenia z fishingiem – czyli łowieniem ryb. Przestępcy, podobnie jak wędkarze, stosują bowiem odpowiednio przygotowaną „przynętę”. Do tego wykorzystują najczęściej sfałszowane e-maile i SMS-y. Próby wyłudzenia poufnych informacji, takich jak hasła czy dane finansowe, poprzez podszywanie się pod zaufane źródła.

Do ataków typu phishing wykorzystywane są wszystkie formy komunikacji elektronicznej:
- wiadomości e-mail
- SMS-y
- wiadomości na komunikatorach (np. WhatsApp)
- wiadomości prywatne w serwisach społecznościowych (np. na Instagramie)
- rozmowy telefoniczne

WAMA SMART LAB
EKONOMIA WODY
WARMIŃSKO-MAZURSKIE

Ataki phishingowe

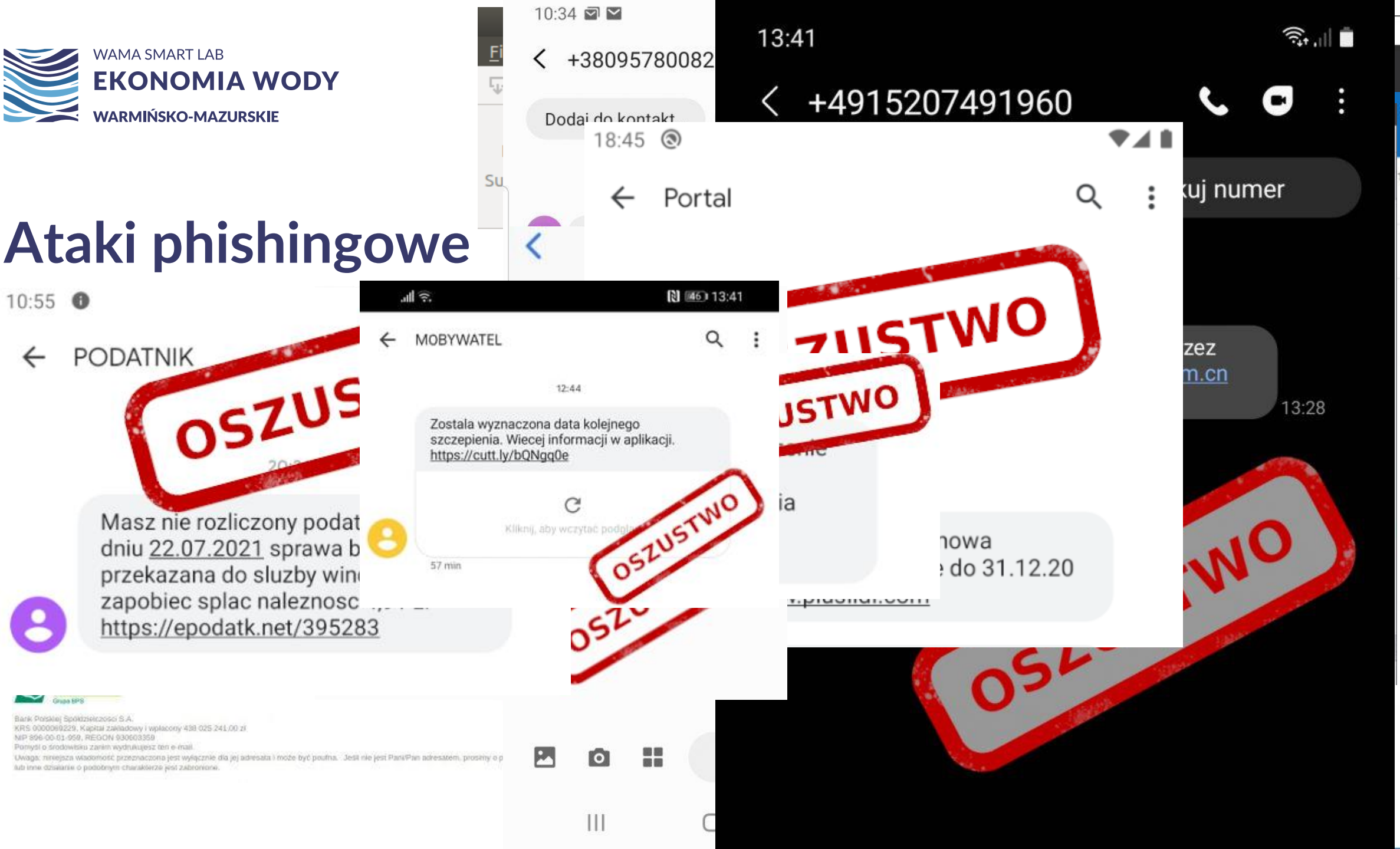
Celem ataku phishingowego nie jest sprzęt czy oprogramowanie, ale sam człowiek.
Atakujący korzysta najczęściej z autorytetu osoby lub instytucji.
Treść wiadomości najczęściej ma za zadanie wzbudzić w odbiorcy silne emocje takie jak strach czy wymusić pośpiech.

Dane to:

- podanie danych logowania do banku na spreparowanej stronie WWW
- podanie danych karty płatniczej / kredytowej
- wpisanie loginu i hasła logowania do skrzynki pocztowej
- pobranie pliku ze złośliwym oprogramowaniem

WAMA SMART LAB
EKONOMIA WODY
WARMIŃSKO-MAZURSKIE

Ataki phishingowe



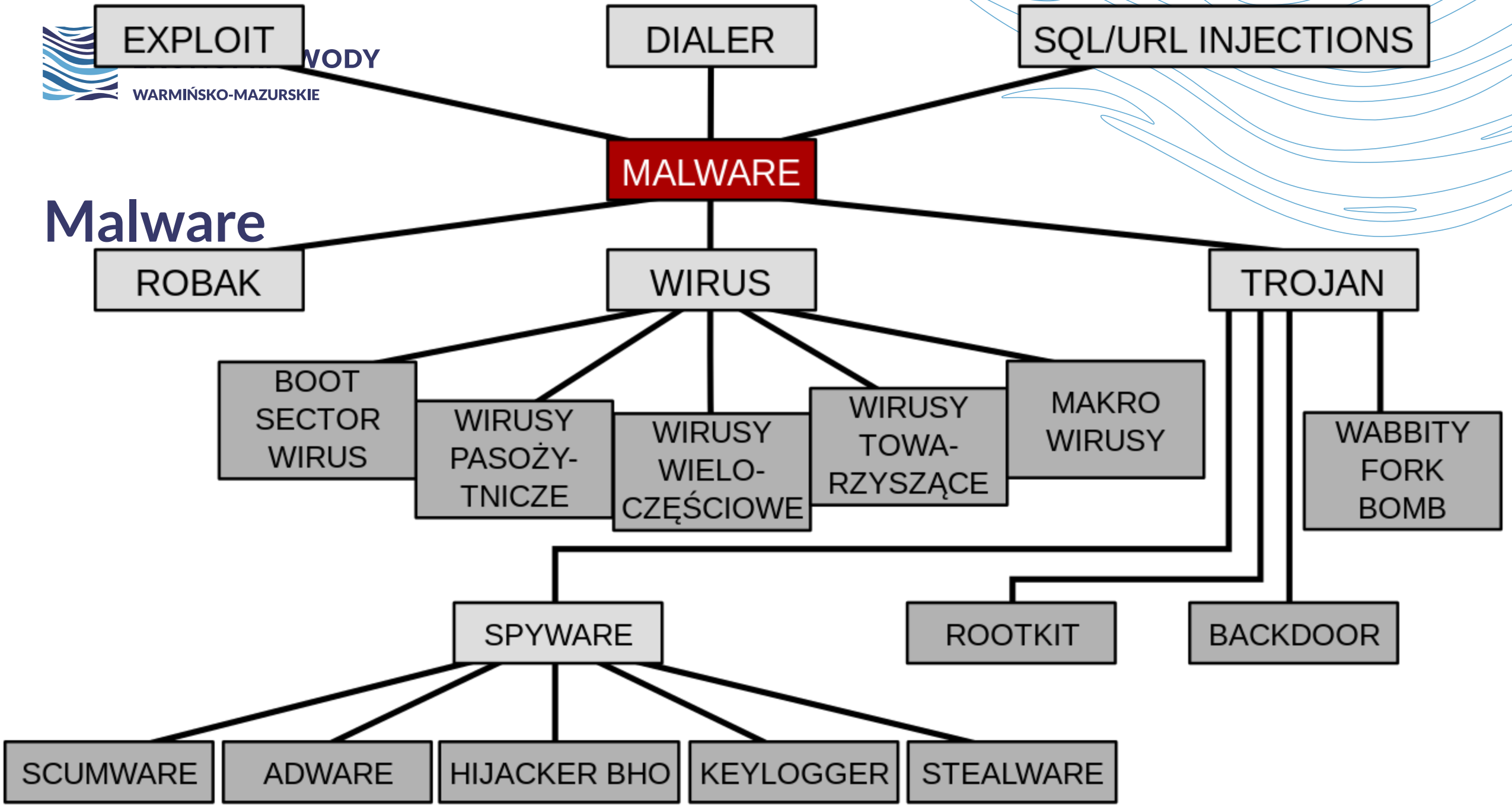
WAMA SMART LAB
EKONOMIA WODY
WARMIŃSKO-MAZURSKIE

Malware

Złośliwe oprogramowanie, takie jak wirusy, trojany czy ransomware, może zainfekować systemy MŚP, prowadząc do utraty danych lub blokady dostępu do nich. Mianem malware określa się wyłącznie oprogramowanie, które zostało przeznaczone do złych celów i działa wbrew oczekiwaniom użytkownika; określenie to nie obejmuje aplikacji, które mogą wyrządzić niezamierzoną szkodę z powodu jakiejś niedoskonałości.

WODY
WARMIŃSKO-MAZURSKIE

Malware



WAMA SMART LAB
EKONOMIA WODY
WARMIŃSKO-MAZURSKIE

Braki w aktualizacjach

Nieaktualne oprogramowanie i brak regularnych aktualizacji systemów operacyjnych i aplikacji może otwierać furtki dla ataków. Cyberprzestępcy często wykorzystują znane luki w zabezpieczeniach. Dzięki częstym aktualizacjom oprogramowania możecie czuć się bezpiecznie, korzystając z aplikacji bankowych czy innych programów przechowujących dane osobowe lub istotne informacje.

WAMA SMART LAB
EKONOMIA WODY
WARMIŃSKO-MAZURSKIE

Słabe hasła

Używanie słabych lub łatwo zgadywal
do systemów. Bezpieczne hasło to poc
w cyfrowym świecie jest najważniejs
trudne w złamaniu przez cyberprzestę

. To ułatwia atakującym dostęp
bezpieczeństwo naszych danych
l tym, jak stworzyć silne hasło,
dstawowych zasad.

Top 10 najpopularniejszy wybieranych przez Polak

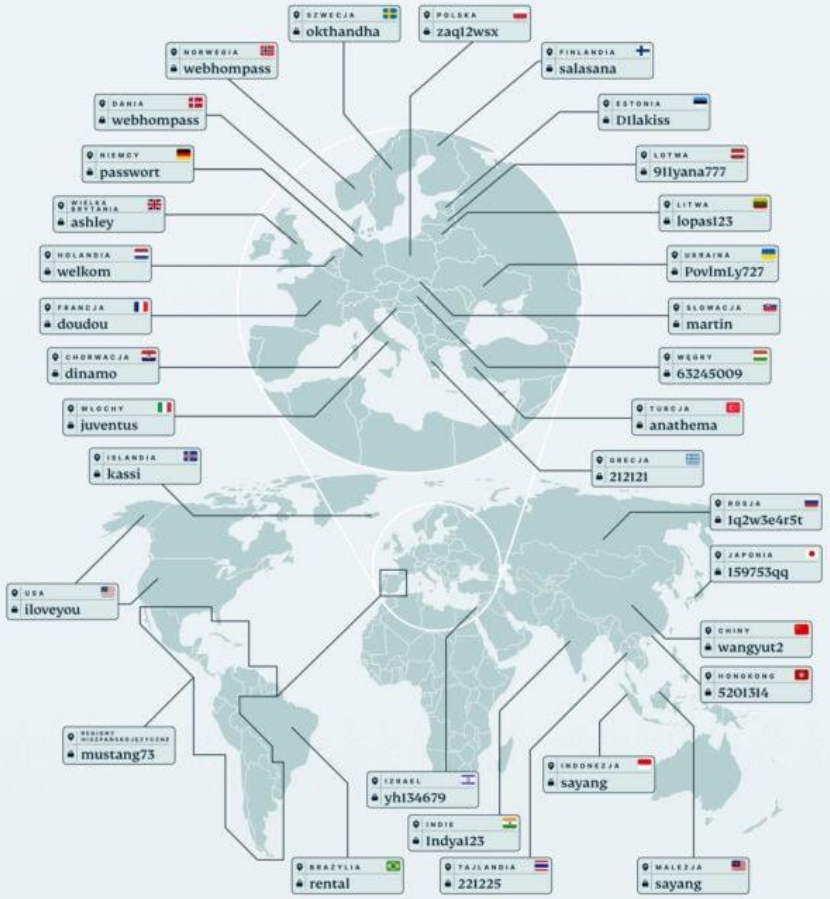
1. 123456	6. polska
2. qwerty	7. 1234
3. zaq12wsx	8. lol123
4. 123456789	9. mateusz
5. 12345	10. 111111

Źródło: Ata Hakçıl

CIEKAWOSTKA
40% spośród 150 najp
haseł zawiera imiona,
jak i żeńskie

Najpopularniejsze hasła na świecie

Słabe hasła są problemem wszędzie - ale występują w różnych formach w zależności od lokalizacji i języka. Oto kilka haseł najczęściej używanych w różnych krajach.



„Na podstawie badań Aty Hakçıl; SafetyDetectives dla USA; Scattered Secrets dla Holandii. Dane niektórych krajów są wywnioskowane na podstawie statystyk związanych z językiem."

ExpressVPN

WAMA SMART LAB
EKONOMIA WODY
WARMIŃSKO-MAZURSKIE

Nieaktualne oprogramowanie antywirusowe i antymalware

Brak odpowiednich narzędzi do wykrywania i usuwania złośliwego oprogramowania może powodować duże zagrożenie.

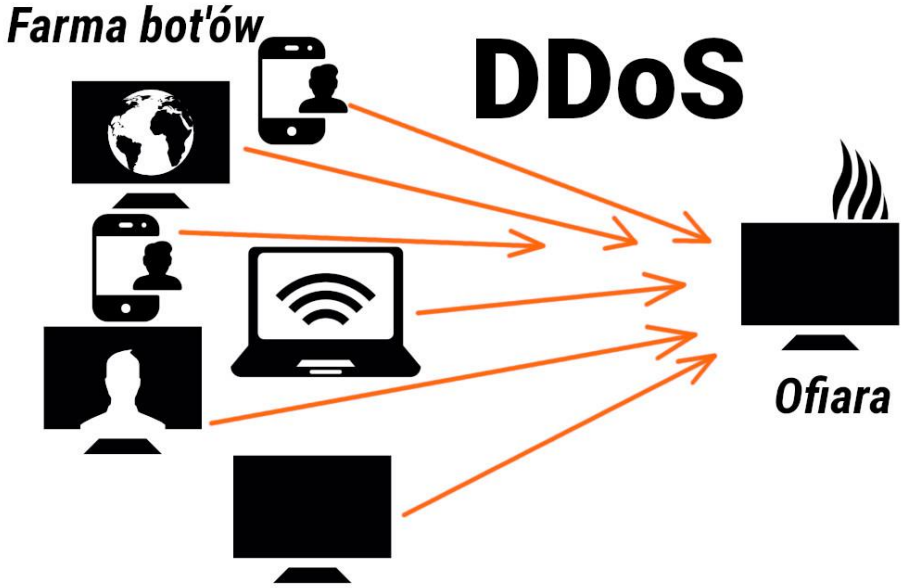
Brak szkoleń dla pracowników

Nieświadomi pracownicy mogą stać się wektorami ataku. Brak świadomości w zakresie cyberbezpieczeństwa może prowadzić do naruszeń.

WAMA SMART LAB
EKONOMIA WODY
WARMIŃSKO-MAZURSKIE

Ataki DDoS (Distributed Denial of Service)

Ataki typu DDoS mogą paraliżować dostępność usług online firmy, co może prowadzić do strat finansowych. Cel zajęcie wszystkich dostępnych i wolnych zasobów komputera. Takie działanie cyberprzestępców ma uniemożliwić korzystanie z urządzenia i dostępnych na nim zasobów, a co za tym idzie – blokować funkcjonowanie usługi online (np. strony internetowej czy poczty e-mail znajdującej się na hostingu).



Zagrożenia związane z dostawcami

Osoby nieuprawnione lub byli pracownicy mogą próbować uzyskać dostęp do systemów firmy, co naraża poufne informacje na Zewnętrzni dostawcy oprogramowania lub usług mogą stanowić ryzyko, jeśli nie zapewnią odpowiednich standardów bezpieczeństwa.

International Software Testing Qualifications Board
– Tester zabezpieczeń
– Inżynier automatyzacji testów
– Tester bazujący na modelu
– Testy użyteczności
– Tester oprogramowania dla branży motoryzacyjnej
– Tester branży hazardowej
– Testowanie aplikacji mobilnych
– Testowanie wydajności
– Testowanie akceptacyjne

WAMA SMART LAB
EKONOMIA WODY
WARMIŃSKO-MAZURSKIE

Zagrożenia związane z mobilnością

Wprowadzenie BYOD (Bring Your Own Device) może zwiększyć ryzyko, jeśli urządzenia pracowników nie są odpowiednio zabezpieczone.

WAMA SMART LAB
EKONOMIA WODY
WARMIŃSKO-MAZURSKIE

Cyberprzestępczość ukierunkowana na MŚP

W niektórych przypadkach cyberprzestępcy specjalizują się w atakach na MŚP, zakładając, że są one mniej zabezpieczone niż większe korporacje.

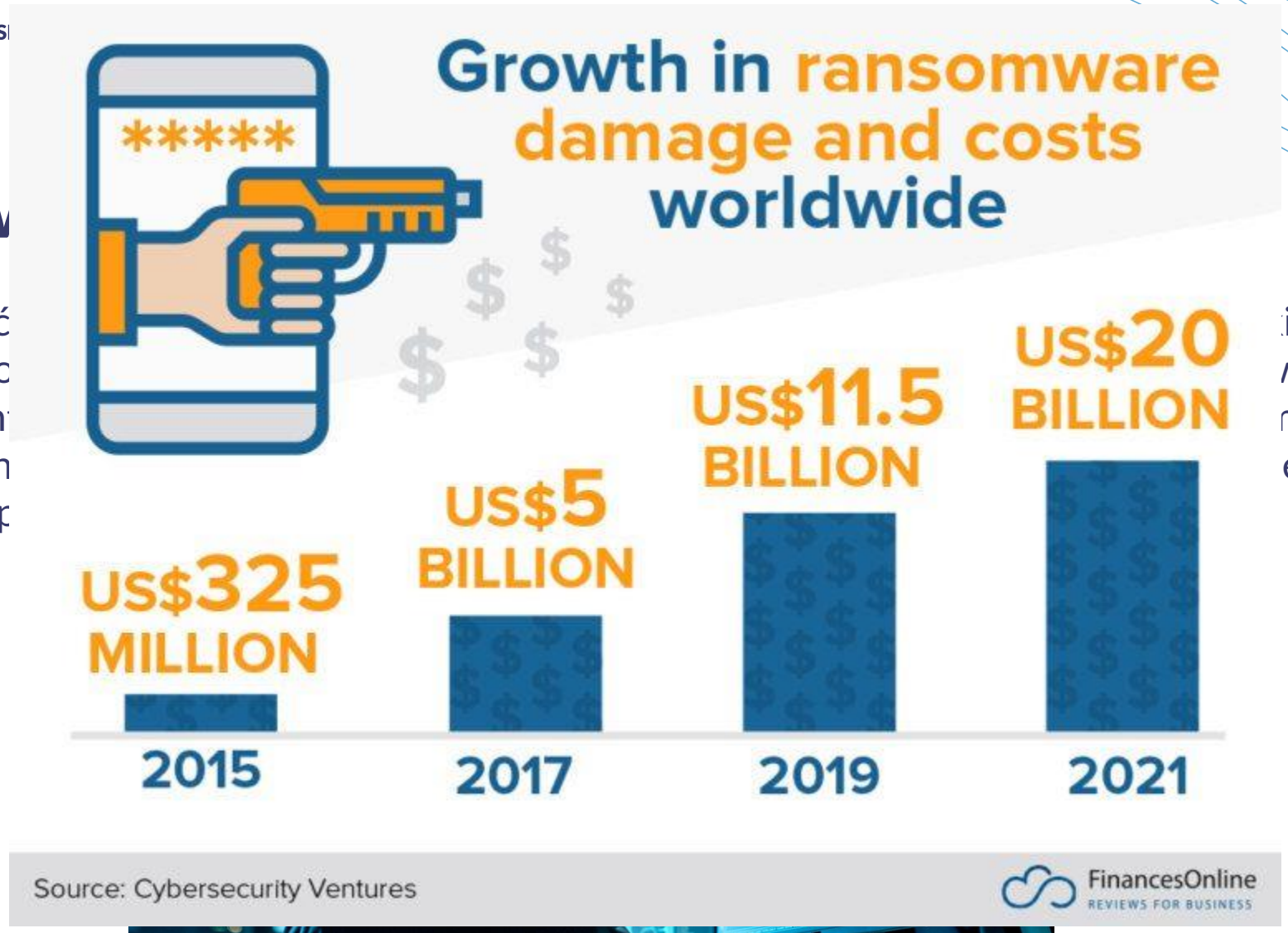
WAMA SMART LAB
EKONOMIA WODY
WARMIŃSKO-MAZURSKIE

Brak strategii zarządzania incydentami

MŚP często nie mają odpowiednio przemyślanej strategii na wypadek naruszenia bezpieczeństwa, co może prowadzić do poważnych konsekwencji.

Podsumow

Aby zminimalizować ie jak firewall, systemy antywirusc a oraz plany zarządzania incyden nonitorowanie sieci w poszukiwan ekspertami w dziedzinie cyberbezp



WAMA SMART LAB
EKONOMIA WODY
WARMIŃSKO-MAZURSKIE

Firma Bezpieczna Cyfrowo – nowy program wzmacniania cyberbezpieczeństwa w MŚP

Cele programu Firma Bezpieczna Cyfrowo

- Rozwój kompetencji cyfrowych wśród polskich przedsiębiorców, ze szczególnym uwzględnieniem cyberbezpieczeństwa.
- Podniesienie poziomu bezpieczeństwa MŚP oraz stabilności obrotu gospodarczego w Polsce.
- Upowszechnienie i wdrożenie nowego standardu cyberbezpieczeństwa w firmach.

Więcej informacji o programie znajdziesz na stronie https://firmabezpiecznacyfrowo.pl/organizatorzy.

WAMA SMART LAB

EKONOMIA WODY

WARMIŃSKO-MAZURSKIE

Cyberbezpieczeństwo w małych i średnich przedsiębiorstwach – *przegląd zagrożeń. Pytania ?*

mł. insp. dr inż. Michał Bukowski

+48 47 733 52 78 / +48 728 466 320

m.bukowski@wspol.edu.pl

Dyrektor Instytutu Służby Kryminalnej Wydziału Bezpieczeństwa i Nauk Prawnych

Akademii Policji w Szczytnie

Fundusze Europejskie Program Regionalny

Rzeczpospolita Polska

WARMIA MAZURY Zdrowe życie, czysty zysk

Unia Europejska Europejski Fundusz Społeczny