Czy technologie XX wieku mają szanse z cyberprzestępczością XXI wieku?

Badanie „Cyberbezpieczeństwo Firm"

Warszawa, 2 marca 2017

The better the question. The better the answer.
The better the world works.

EY
Building a better working world

6,5 mld

urządzeń podpiętych do Internetu w 2016 roku

Źródło: Gartner

Liczba urządzeń zaatakowanych przez malware bankowy

Źródło: Kaspersky Security Bulletin 2016

117

DNI złośliwe oprogramowanie znajdowało się na serwerach polskiego regulatora instytucji finansowych

2016-09-07 – 2017-02-01

NAWET

90

DNI mógł trwać incydent w jednym z polskich banków

styczeń 2015 – kwiecień 2015

ŚREDNIO

469

DNI zajmuje europejskim firmom wykrycie incydentu

Źródło: Mandiant M-trends 2016 EMEA Edition

Czy polskie firmy są bezpieczne?

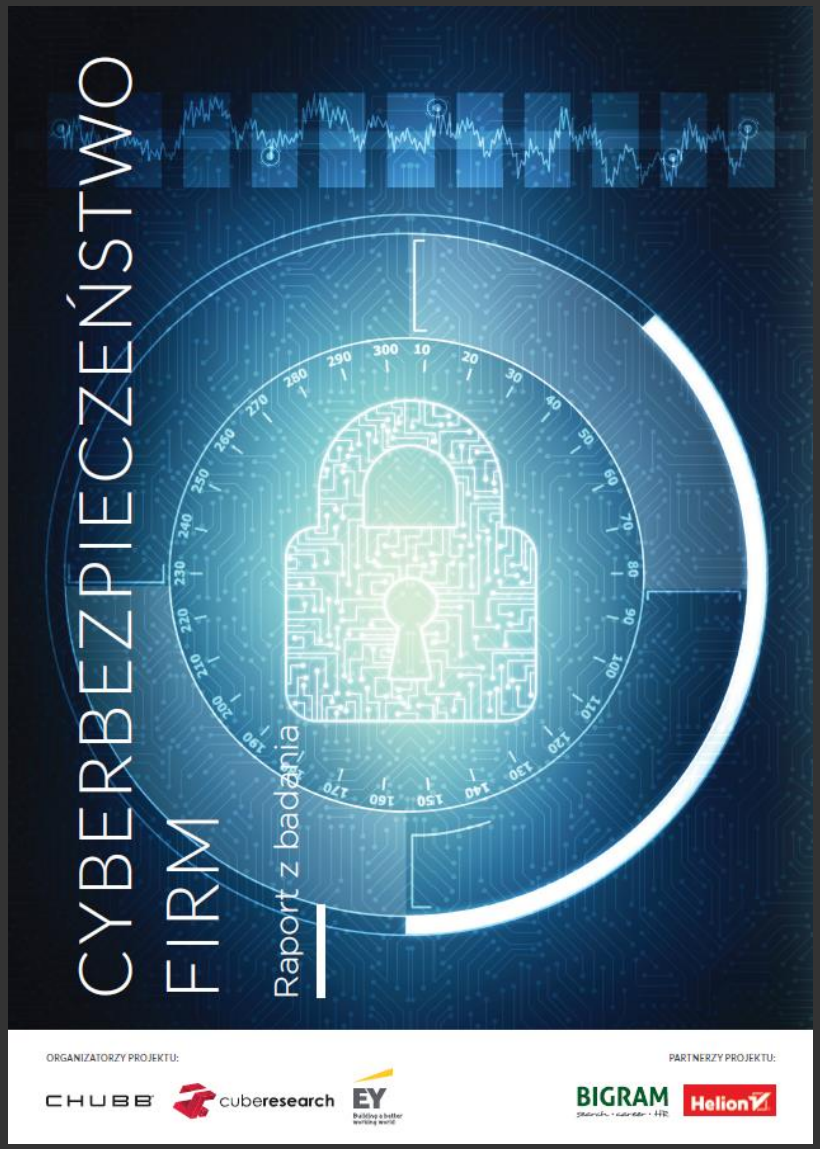
Jak dbamy o aktualność i adekwatność naszych zabezpieczeń?

Czy nasza struktura i organizacja odpowiada ciągle zmieniającym się realiom?

Jak szybko jesteśmy w stanie wykryć incydent bezpieczeństwa?

Kiedy ja zostanę zaatakowany?

Jak reagować w przypadku ataku?

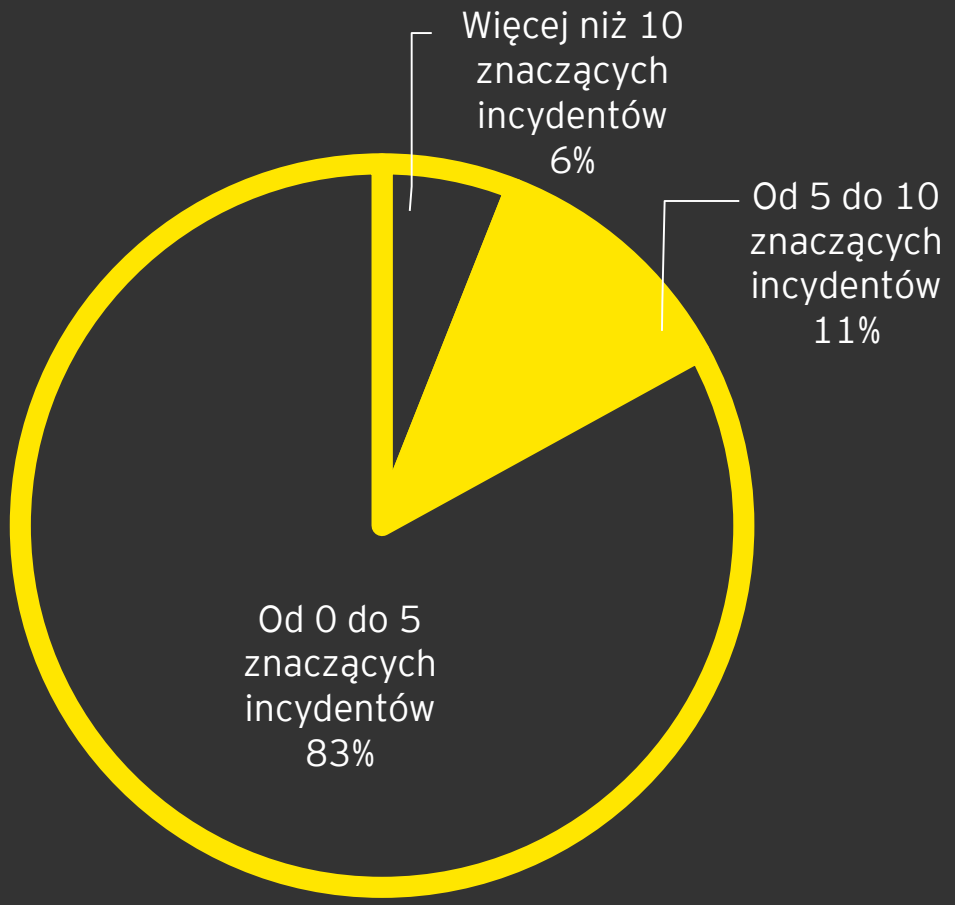


Zasadniczym celem badania było uzyskanie aktualnych danych związanych z tematem cyberbezpieczeństwa firm. Czy firmy zdają sobie sprawę ze stojących przed nimi wyzwań w zakresie zapewnienia cyberbezpieczeństwa? Czy metody i procedury, które stosują pozwalają im spać spokojnie? Czy pracownicy rzeczywiście stanowią największe zagrożenie dla cyberbezpieczeństwa i co zrobić, żeby ich negatywną rolę zminimalizować?

Badanie składało się z dwóch części – badania zasadniczego gdzie zebraliśmy odpowiedzi 350 osób na co dzień zajmujących się problematyką cyberbezpieczeństwa firm, oraz badania dodatkowego zrealizowanego na 500 pracownikach firm.

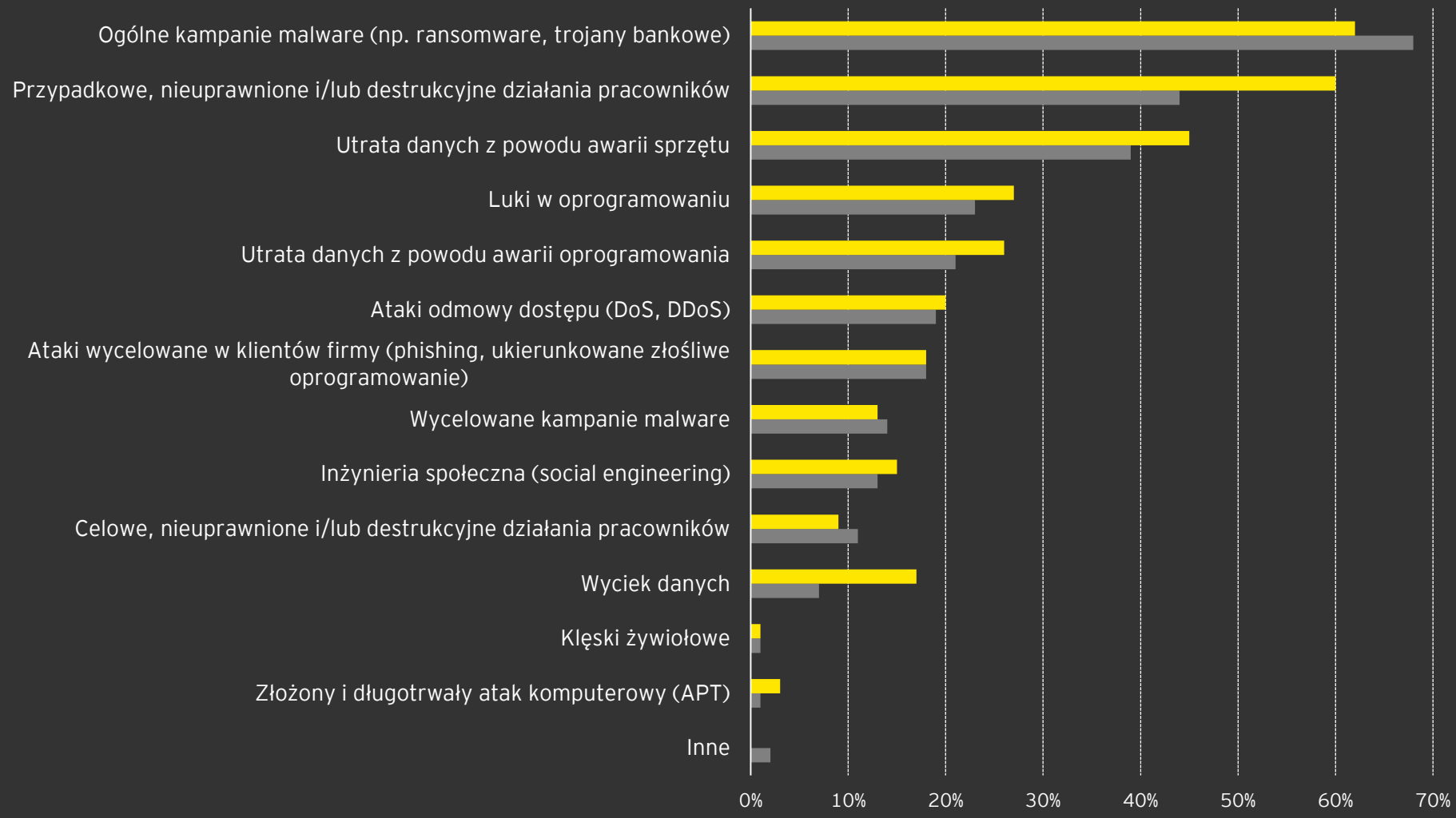
Badanie zrealizowano w listopadzie 2016 na próbie 350 firm.

Ile incydentów bezpieczeństwa odnotowali Państwo w ciągu ostatnich 12 miesięcy?



Z jakiego typu incydentami mieli Państwo do czynienia?

Które z wymienionych niżej zagrożeń ocenia Pan(i) jako najbardziej istotne z punktu widzenia Państwa firmy?



64%

firm objętych badaniem uważa **PRACOWNIKÓW** za najczęstszą przyczynę incydentów

29%

pracowników **NIE ZNA** obowiązujących procedur bezpieczeństwa IT

25%

pracowników uważa, że **BYŁO OBIEKTEM ATAKU** cybernetycznego

72%

firm w trakcie szkoleń bezpieczeństwa ogranicza się wyłącznie do **WYKŁADU**

53%

firm **NIE WDROŻYŁO** rozwiązania mierzącego efektywność przeprowadzonych szkoleń

41%

pracowników **NIGDY** nie odbyło szkolenia z zakresu bezpieczeństwa

36%

firm zdecydowało się na **PODNIESIENIE** budżetu na cyberbezpieczeństwo w zeszłym roku

36%

firm zdecydowało się na **PODNIESIENIE** budżetu na cyberbezpieczeństwo w zeszłym roku

16%

firm dysponuje **DOKŁADNYM REJESTREM INCYDENTÓW** opisującym przedmiot incydentu, podjęte procedury wyjaśniające i zaradcze oraz wnioski na przyszłość

10%

firm dysponuje **DOKŁADNYMI ANALIZAMI STRAT**, które mogłyby ponieść w wyniku cyberataku

EY

CO **8** **FIRMA** dysponuje zespołem reakcji na incydenty

CO **5** **FIRMA** analizuje trendy związane z cyberbezpieczeństwem (*threat intelligence*)

97%

firm w swoim planie reakcji na incydent **NIE UWZGLĘDNIA** działów nietechnicznych (np. prawny, finansowy, PR)

75%

Respondentów uważa, że bezpieczeństwo jest kompetencją **WYŁĄCZNIE** działu IT

73%

firm dysponuje zespołem **NAJWYŻEJ 3 OSÓB** zajmujących się bezpieczeństwem

uważa, że dysponuje rozwiązaniami umożliwiającymi **WYKRYCIE ZAGROŻEŃ** w swojej infrastrukturze

60%

firm uważa, że dysponuje rozwiązaniami umożliwiającymi **WYKRYCIE ZAGROŻEŃ** w swojej infrastrukturze

50%

w celu zapewnienia bezpieczeństwa korzysta **WYŁĄCZNIE** z antywirusa i firewalla

15%

firm dysponuje innymi środkami bezpieczeństwa niż **PODSTAWOWE***

* - firewall, antywirus, WAF, IDS, IPS

85%

firm **NIE WDROŻYŁO** wszystkich rekomendacji wynikających z ostatniego audytu bezpieczeństwa

76%

firm **NIE PRZEPROWADZA** regularnych testów bezpieczeństwa swojej infrastruktury

41%

firm **NIE TESTUJE** nowych wdrożeń w swojej infrastrukturze

25%

firm **NIGDY** nie przeprowadziło audytu bezpieczeństwa swojej infrastruktury

61%

firm **NIE BLOKUJE** dostępu do zewnętrznych serwisów internetowych (np. wymiany plików)

65%

firm **ZEZWALA** pracownikom na korzystanie z prywatnych urządzeń (*BYOD*)

79%

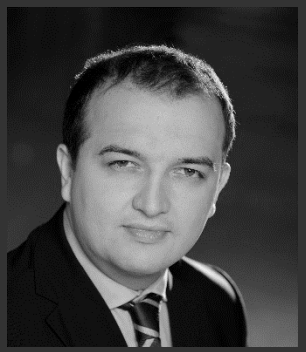
firm **NIE ZABEZPIECZA** logów przed nadpisaniem przez użytkowników wysoko uprawnionych (np. administratorów)

86%

firm **NIE JEST W STANIE W PEŁNI** monitorować czynności pracowników w infrastrukturze

Zapraszamy do kontaktu!

Aleksander Ludynia
Starszy Menedżer
+48 32 760 7876
+48 519 511 516
aleksander.ludynia@pl.ey.com



Grzegorz Idzikowski
Menedżer
+48 22 557 8845
+48 519 511 433
grzegorz.idzikowski@pl.ey.com