Najnowsze wyzwania

w obszarze cyberbezpieczeństwa

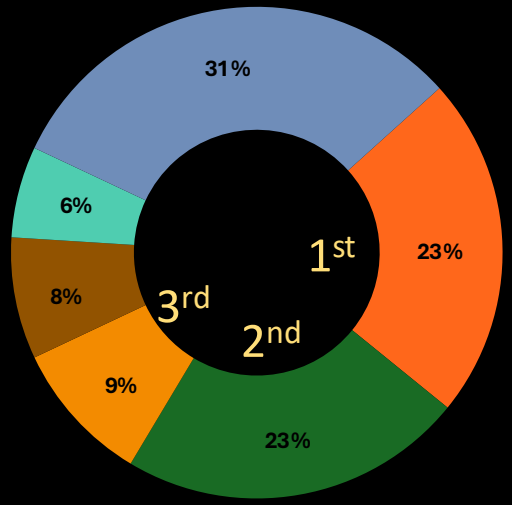
w świetle dyrektywy NIS2

Małgorzata Domagała

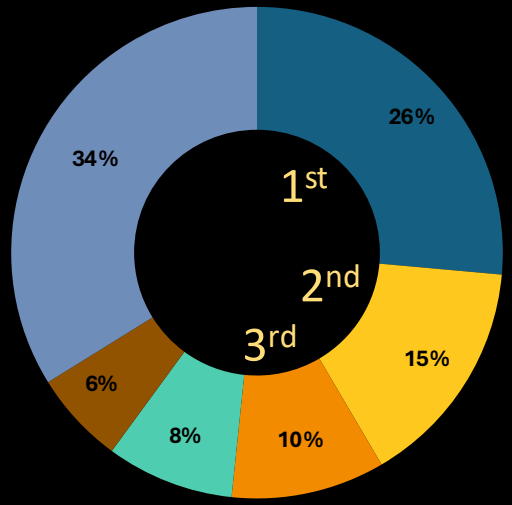
Złośliwe oprogramowanie, ransomware i phishing e-mailowy pozostają trzema najbardziej rozpowszechnionymi metodami ataków zarówno w europejskim, jak i polskim krajobrazie cyberbezpieczeństwa

Metody ataku – wszystkie atakowane sektory

Europe



Poland



- Malware
- Ransomware
- Email Phishing
- Denial of Service
- Supply Chain Attack
- Reconnaissance
- Web Application Attack
- Other

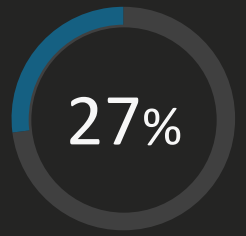
***Industries below 5% grouped under «Other» category**

- *Supply Chain Attack, Pretexting, Command & Control, Legitimate Tool, Web Application Attack*

Source: Mastercard Cyber Insights Data. Based on data for the period January 2023 - June 2024

Najpopularniejsze taktyki, techniki i procedury

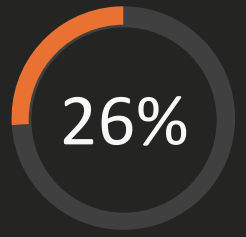
Malware



większość ataków na **instytucje rządowe**

Europejska średnia: 19%

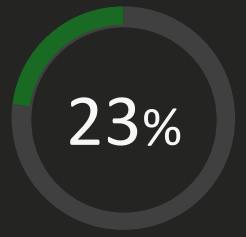
Ransomware



większość ataków na **instytucje rządowe**

Europejska średnia: 18%

Email Phishing



większość ataków na **instytucje rządowe**

Europejska średnia: 17%

DLACZEGO MASTERCARD & CYBER SECURITY?

Ekosystem cyber- zaczyna się TUTAJ

Mastercard znajduje się w centrum światowego handlu, łącząc **1 miliard ludzi z gospodarką cyfrową.**

143.2mld

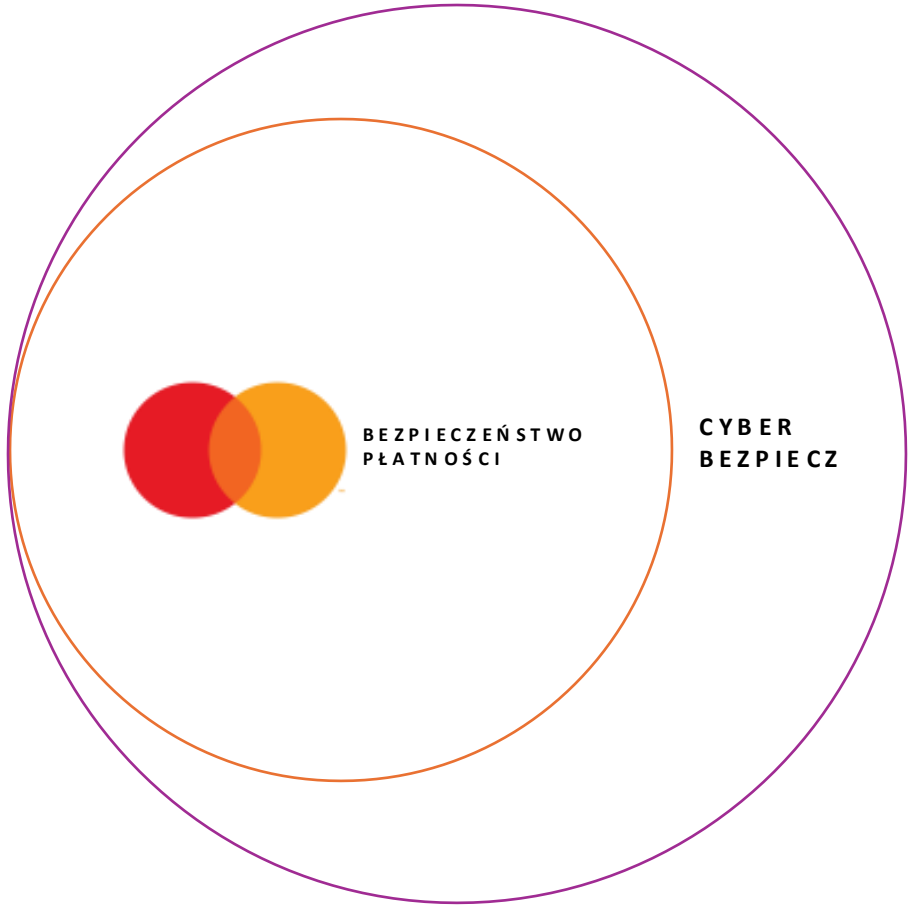
Transakcji przetworzonych w 2023

3.3mld

Kart globalnie

100m

Punktów akceptacji



Warstwa cyberbezpieczeństwa wzmacnia bezpieczeństwo płatności i nie tylko, **w cyfrowym świecie zależnym od zaufania.**

147zb

data globally in 2024

$7.9t

E-commerce do 2027

5.4b

Connected internet users[1]

1. Internet Usage Statistics in 2024. Forbes.

DLACZEGO MASTERCARD & CYBER SECURITY?

Musimy zabezpieczyć każdą interakcję poza transakcją – we wszystkich branżach – na wszystkich poziomach łańcucha dostaw.

3,420+

Banków i instytucji finsowych monitorowanyc

13m+

Merchantów monitorowanych

40+

Branż

Mastercard Propriety Data. 2024

2x

Liczba organizacji zarządzających ryzykiem ponad 250 relacji z osobami trzecimi podwoiła się w 2023 r. w porównaniu z 2020r

75%

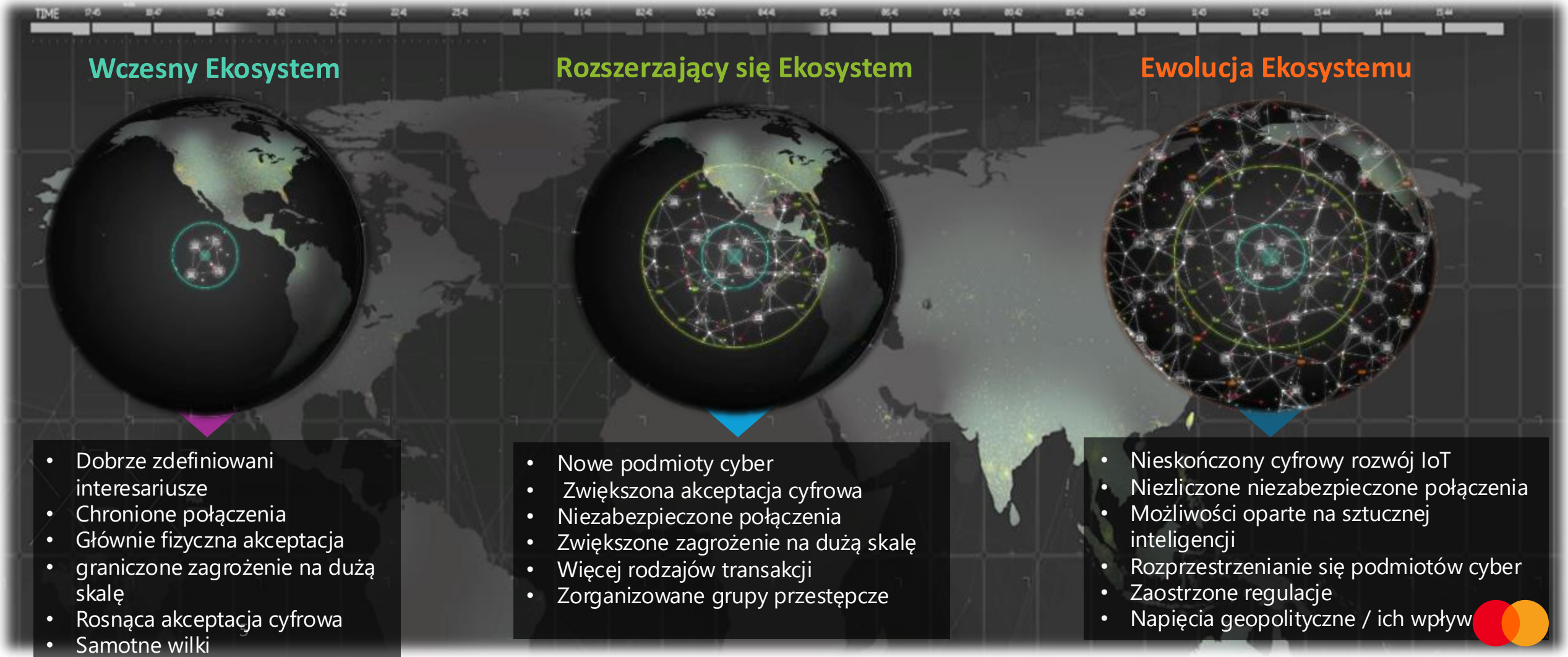
Powiązania biznesowe występują na czwartym i piątym poziomie łańcucha dostaw. 2

50k+

Monitorowane są relacje między czwartą a n-tą stroną.

Source[1]: The State of Third-Party Risk Management: 2024 Outlook. RiskRecon by Mastercard. Source[2]: Risk to the Nth-Party Degree: Parsing the Tangled Web. RiskRecon By Mastercard.

Ochrona rozwijającego się ekosystemu idzie dziś poza ochranianianie transakcji



MASTERCARD CYBERSECURITY

Teraz wnosimy naszą wieloletnią wiedzę specjalistyczną do szerszego ekosystemu, ponieważ wierzymy, że nasze rozwiązania oparte na sztucznej inteligencji powinny być dostępne dla wszystkich organizacji, niezależnie od ich wielkości, branży, wiedzy z zakresu cyberbezpieczeństwa czy relacji sieciowych z nami.

OCENIĆ
ryzyko

OCHRONIĆ
przed atakami

ZORGANIZOWAĆ
ekosystem zaufania

NIS 2: Podmioty Objęte Regulacją

1 Średnie i Duże Firmy

Z sektorów wymienionych w dyrektywie.

2 Łańcuchy Dostaw

Firmy będące częścią łańcuchów dostaw kluczowych sektorów.

3 Instytucje Publiczne

Administracja publiczna i kluczowe usługi państwowe.

Wzmocnienie Cyberbezpieczeństwa

1

Analiza Ryzyka

Identyfikacja zagrożeń i podatności systemów.

2

Implementacja Zabezpieczeń

Wdrożenie odpowiednich środków technicznych i organizacyjnych.

3

Ciągłe Monitorowanie

Stały nadzór nad bezpieczeństwem sieci i systemów.

KARY za niedopełnienie zasad: do 10 mln euro lub 2% światowych obrotów

Obowiązek Zgłaszania Incydentów

1

Wykrycie Incydentu

Identyfikacja poważnego naruszenia bezpieczeństwa.

2

Raportowanie

Zgłoszenie do odpowiednich organów w określonym czasie.

3

Analiza i Reakcja

Współpraca z organami w celu minimalizacji skutków.

Przygotowanie do NIS2

Audyt Bezpieczeństwa

Ocena obecnego stanu zabezpieczeń.

Wdrożenie Zabezpieczeń

Implementacja niezbędnych środków ochrony.

Szkolenia Pracowników

Podnoszenie świadomości i kompetencji w zakresie cyberbezpieczeństwa.

Ciągłe Doskonalenie

Regularne aktualizacje i testy systemów bezpieczeństwa.

Przygotowanie i adopcja NIS2

Obszar	Opis	Wymagania
1. Zarządzanie ryzykiem ICT	Zarządzanie ryzykiem ICT w celu nadążania za szybko zmieniającym się krajobrazem zagrożeń cybernetycznych i dostosowania strategii biznesowych	• Ocena ryzyka związanego z ICT • Klasyfikacja/priorytetyzacja procesów • Ocena wpływu na działalność • Program i szkolenia w zakresie odporności cyfrowej
2. Raportowanie incydentów	Proces zarządzania incydentami związanymi z ICT, w tym wskaźniki wczesnego ostrzegania, w celu wykrywania incydentów związanych z ICT, zarządzania nimi i powiadamiania o nich	• Klasyfikacja i raportowanie incydentów • Testy • Komunikacja z organami • Ilościowe określanie kosztów strat spowodowanych incydentem
3. Testowanie odporności	Kompleksowy program testowania operacyjnej odporności cyfrowej oraz testowanie narzędzi, systemów i procesów ICT	• Program testowania odporności • Podejście oparte na analizie ryzyka • Niezależne, ciągłe testy • Metodyki walidacji
4. Ryzyko 3rd Party	Zarządzanie ryzykiem ze strony zewnętrznych dostawców usług ICT jako integralny składnik ryzyka związanego z ICT w ramach zarządzania ryzykiem związanym z ICT	• Proces zarządzania ryzykiem ze strony trzeciej • Podejście do onboardingu dostawców • Definicja poziomów wielu dostawców • Ciągłe testowanie

Produkty MC

- CYBERQUANT mastercard
- CYBERINSIGHTS mastercard
- riskrecon mastercard
- CYBERFRONT mastercard
- Threat Scan
- Systemic Risk Assessment
- **Cybersecurity Advisory**

Source: Mastercard, Mastercard Advisors analysis

Statement of Confidentiality and Disclaimer

Information in this presentation or in any report or deliverable provided by MasterCard in connection herewith relating to the projected impact on your financial performance, as well as the results that you may expect generally are estimates only. No assurances are given that any of these projections, estimates or expectations will be achieved, or that the analysis provided is error-free. You acknowledge and agree that inaccuracies and inconsistencies may be inherent in both MasterCard's and your data and systems, and that consequently, the analysis may itself be somewhat inaccurate or inconsistent. The information, including all forecasts, projections, or indications of financial opportunities are provided to you on an "AS IS" basis for use at your own risk. Mastercard will not be responsible for any action you take as a result of this presentation, or any inaccuracies, inconsistencies, formatting errors, or omissions in this presentation.