PRZEWODNIK TECHNICZNY

Bitdefender

Bitdefender (EDR)

Security

Dlaczego zespoły ds. bezpieczeństwa potrzebują EDR

www.bitdefender.pl

Spis treści

Ochrona punktów końcowych: niezbędna, lecz niepozbawiona ograniczeń

Zapobieganie i blokowanie nie wystarczą

Dzisiejsze rozwiązania typu Endpoint Protection (EPP) od czołowych producentów rozwiązań bezpieczeństwa są na coraz wyższym poziomie. W porównaniu z wcześniejszymi rozwiązaniami, nowoczesne narzędzia EPP zatrzymują więcej złośliwego oprogramowania i bardziej zróżnicowane rodzaje zagrożeń niż kiedykolwiek wcześniej. Najlepsi producenci wdrożyli sztuczną inteligencję (AI), uczenie maszynowe (ML) i adaptacyjną heurystykę, które wykraczają daleko poza statyczne i łatwe do obejścia "sygnatury wirusów" z przeszłości.

Wykrywanie przed uruchomieniem, blokowanie w chwili uruchomienia, a nawet zakończenie po uruchomieniu są obecnie powszechnymi funkcjami najlepszych produktów EPP. Ogólnie zmniejsza się liczba fałszywych alarmów, poprawia się szybkość i precyzja wykrywania, dostępne są też lepsze objaśnienia dotyczące wykrytych zagrożeń i ich przyczyn. Jednak EPP jako kategoria produktów ma fundamentalne ograniczenia, które każdy administrator powinien mieć na uwadze. Kiedy na szali jest bezpieczeństwo Twojej firmy, nie możesz stracić z oczu tego, co jest niewidoczne dla narzędzi Endpoint Protection.

Dlaczego ochrona punktów końcowych bywa niewystarczająca

Zapobieganie atakom poprzez wykrywanie i blokowanie na samym początku każdego ataku wydaje się być idealnym rezultatem, który chciałby osiągnąć każdy zespół InfoSec, ale jak pokazuje historia od czasów pierwszych wirusów komputerowych w połowie lat 80-tych, jest to cel trudny do osiągnięcia. Zapobieganie nigdy nie było możliwe w 100%, a " idealne zabezpieczenie" jest praktycznie nieosiągalne. Ataki bezplikowe i exploity przeglądarek nie wykorzystują plików, które można zablokować, a wiele zaawansowanych wieloetapowych i wielowektorowych ataków przebiega w sposób, który czyni je wyjątkowo trudnymi, jeśli nie niemożliwymi do powstrzymania. Ograniczenia EPP obejmują w szczególności:

- **Zbyt mało, za późno:** Wykrycie potrafi nastąpić dopiero wówczas, gdy złośliwe oprogramowanie osiągnie całkowity lub połowiczny sukces, a maszyna docelowa została zainfekowana przy zablokowaniu tylko jednego z elementów ataku.
- **Brakujące powiązania:** Wiele alarmów może być generowanych przez EPP bez oczywistych wspólnych wątków łączących je ze sobą. Analitycy nie mogą zobaczyć kompletnych incydentów lub łańcuchów powiązanych zdarzeń.
- **Brakujące powiązania:** Wiele alarmów może być generowanych przez EPP bez wyraźnych powiązań między nimi. Analitycy nie mogą zobaczyć pełnego obrazu zdarzenia lub łańcucha powiązań.

Dlaczego warto mieć EDR w swoim arsenale zabezpieczeń?

Usunięcie istotnych luk w zabezpieczeniach

Ochrona punktów końcowych jest niezbędna dla zachowania zgodności z normami oraz do ochrony przed złośliwym oprogramowaniem i typowymi zagrożeniami, jednak nie jest wystarczająca do obrony przed zaawansowanymi, złożonymi lub ukierunkowanymi atakami. Jeśli Państwa własność intelektualna, dane PII/PHI, dane klientów lub dane finansowe są narażone na ryzyko, EDR nie jest zbędnym luksusem — jest koniecznością.

Niewystarczająca ochrona przed zaawansowanymi zagrożeniami

Sama ochrona punktów końcowych zazwyczaj nie zapewnia wystarczającej ochrony przed zaawansowanymi zagrożeniami. Złożone ataki często rozpoczynają się od nieszkodliwych lub standardowych oznak aktywności - otwarcia dokumentu, nawiązania połączenia zdalnego, pobrania zasobu z internetu itp. Dopiero później pojawiają się sygnały mówiące o podejrzanym lub szkodliwym działaniu.

Brak możliwości analizy i reagowania na alerty

Ochrona punktów końcowych generuje wiele alertów, jednak nie uwzględnia każdego elementu danego ataku. Mimo, że każdy alert reprezentuje realne zagrożenie, które zostało zablokowane, mogą być konieczne dalsze kroki w celu analizy i podjęcia działań naprawczych, wykraczających poza usunięcie wykrytych niebezpiecznych plików z systemu organizacji. Od czego zatem zacząć?

Powolna reakcja na wykryte zagrożenia

EPP dostarcza niewielu sygnałów wczesnego ostrzegania przed atakiem i nie wprowadza odpowiedniego rozróżnienia na kategorie typu "szkodliwy" i "nieszkodliwy", przy niewielkiej ilości szczegółów dotyczących oceny zagrożenia. Użytkownik może zauważyć nieprawidłowe działanie komputera, inżynier sieciowy może spostrzec nietypowy ruch sieciowy lub skokowy przepływ danych, jednak nie są dostępne żadne szczegóły dotyczące przyczyn takich zdarzeń.

Brak możliwości identyfikacji pierwotnej przyczyny i zapobiegania ponownym atakom

Załóżmy, że Twoje rozwiązanie EPP coś zablokowało. Nie ciesz się jednak przedwcześnie. Czy jesteś przekonany, że powstrzymano cały atak, czy tylko jeden jego element? Czy inne aspekty ataku skutecznie uniknęły wykrycia? Co było źródłem zagrożenia? Skąd się wzięło? Jak zlikwidować tę podatność, aby atak się nie powtórzył?

Brak wglądu w taktyki, technik i procedur (TTP) / wskaźników naruszenia bezpieczeństwa (IOC) stosowane w całej organizacji

Czy było to jednorazowe zdarzenie, czy też ma ono charakter systemowy i dotyczy wielu maszyn w przedsiębiorstwie? Czy atak tego typu lub podobny wystąpił w przeszłości wielokrotnie? Czy atak ma nadal miejsce na innych maszynach w organizacji? Czy możesz zidentyfikować pojedynczy wskaźnik ataku lub zagrożenia i przeszukać pod jego kątem cały system?

Brak zaleceń dotyczących proaktywnego zwiększania poziomu bezpieczeństwa

Jak możesz poprawić swoją politykę bezpieczeństwa i wzmocnić obronę przed przyszłymi atakami? Czy potrafisz zidentyfikować błędną konfigurację systemu operacyjnego, luki w aplikacjach i ludzkie czynniki behawioralne, które zwiększają ryzyko dla Twojej organizacji? Czy po ich zidentyfikowaniu jesteś w stanie zmierzyć i ocenić postępy w zakresie poprawy bezpieczeństwa?

Czynniki warunkujące skuteczność EDR

Oto główne przesłanki ekonomiczne, które przemawiają za wprowadzeniem EDR do arsenału obronnego Twojej organizacji:

- Nie możesz zapewnić 100% ochrony przed zaawansowanymi atakami, które pozwalają intruzom pozostać w Twoich systemach
- Nie można zakończyć podejrzanej aktywności lub odizolować zainfekowanych maszyn po wykryciu potencjalnych wskaźników naruszenia bezpieczeństwa
- Brakuje Ci informacji, na podstawie których można podjąć działania lub wskazówek, jak krok po kroku postępować w przypadku zidentyfikowania naruszenia
- Brak scentralizowanej bazy danych o zagrożeniach dla potrzeb skoordynowania analizy ataków i działań naprawczych we wszystkich systemach
- Nie są Ci znane ryzyka systemowe, na które narażona jest Twoja infrastruktura, ani sposoby proaktywnego zwiększania poziomu bezpieczeństwa."

Zalety samodzielnego rozwiązania EDR

Endpoint Detection and Response wnosi dodatkową wartość i działa niezależnie, oddzielnie i komplementarnie względem ochrony punktów końcowych. Traktując te dwa rozwiązania niczym tandem typu "pas i szelki" chroniący przed najtrudniejszymi atakami, których celem jest uniknięcie pierwszej linii obrony. Możesz też nadal korzystać z dotychczasowego rozwiązania EPP i rozszerzyć swoją ochronę o EDR.

Jak oceniasz swoje narzędzia EPP?

Wszystkie rozwiązania EPP mają wady i zalety oraz pociągają za sobą konieczność kompromisów. Które stwierdzenie najlepiej opisuje Państwa przypadek?

- Jestem zadowolony z mojego rozwiązania EPP, ale dostrzegam jego ograniczenia w zakresie diagnostyki i działań naprawczych
- Jestem niezadowolony z obecnego rozwiązania EPP, ale do końca obowiązywania umowy zostało jeszcze trochę czasu
- Mam wątpliwości co do mojego obecnego rozwiązania EPP, ale wdrożenie innego narzędzia byłoby zbyt kłopotliwe."

Niezależnie od tego jak oceniasz swoje rozwiązanie EPP, zobacz jak samodzielne rozwiązanie EDR może okazać się najprostszym i zarazem najistotniejszym uzupełnieniem Twojego systemu zabezpieczeń. To prostsze i bardziej opłacalne niż mogłoby się wydawać.

Kiedy samodzielne rozwiązanie EDR jest dobrym wyborem?

Osoby zarządzające bezpieczeństwem mogą uznać samodzielne rozwiązanie EDR za istotne uzupełnienie EPP w następujących okolicznościach:

- Analitycy bezpieczeństwa nie mają wglądu w podejrzaną i niebezpieczną aktywność w punktach końcowych i w sieci
- W istniejącym rozwiązaniu EPP brakuje łatwych, przydatnych opcji dodania EDR opartego na chmurze, EDR+EPP lub MDR
- Potrzebna jest zdolność wykrywania i raportowania incydentów, która byłaby możliwa do pogodzenia z dotychczasowym rozwiązaniem EPP
- Poszukiwana jest chmurowa platforma reagowania na incydenty z prostym i lekkim agentem, który jest łatwy do wdrożenia i zarządzania
- Potrzeba uproszczonych, funkcjonalnych schematów postępowania metodą "krok po kroku" dla analizy zagrożeń i naprawy skutków w punktach końcowych

Bitdefender Endpoint Detection and Response

Bitdefender Endpoint Detection and Response zapewnia połączenie detektywistycznych, śledczych i naprawczych mechanizmów bezpieczeństwa, które pozwalają naszym klientom lepiej zrozumieć typowe alerty z systemów zapobiegania. Wykorzystuje najnowsze i aktualne technologie, aby zapewnić większą widoczność oraz zbierać i skorelować informacje o zagrożeniach. Jednocześnie stosuje analitykę i automatyzację do wykrywania podejrzanych zdarzeń.

Widoczność TTP atakujących

Bitdefender Endpoint Detection and Response dostarcza zaawansowanych funkcji wykrywania i reagowania na ataki, których zespoły ds. bezpieczeństwa nie mają do dyspozycji w konwencjonalnych narzędziach ochrony punktów końcowych. Tradycyjne produkty nie zapewniają wglądu w taktyki, techniki i procedury wykorzystywane do przeprowadzania ataków na stosowane przez nie systemy. Nie dostarczają również analitykom wskazówek dotyczących konkretnych kroków zaradczych, jakie należy podjąć, ani narzędzi niezbędnych do bezpośredniego reagowania na te ataki.

Techniki MITRE ATT&CK

Mapowanie w oparciu o globalny standard bezpieczeństwa, aby mieć wgląd w wykryte zdarzenia i indywidualne alerty dla każdej fazy ataku, w tym: wykonania (Execution), uzyskania trwałej obecności (Persistence), eskalacji uprawnień (Privilege Escalation), omijania zabezpieczeń (Defense Evasion), rozpoznanie uwierzytelnionego dostępu (Credential-led Access Discovery), ruch boczny (Lateral Movement), gromadzenie danych (Collection), zdalna kontrola (Command & Control) oraz eksfiltracja (Exfiltration). Przy zastosowaniu innych narzędzi, które również mapują techniki MITRE ATT&CK, otrzymasz kompletny obraz ataku, wraz z wszelkimi pozostałymi "lukami" w widoczności lub zasięgu, które mogą wymagać jeszcze naprawy.

Wyszukiwanie i korelacja IOC / IOA

Jakich znaków ostrzegawczych należy szukać, aby sprawdzić, czy maszyna została zaatakowana lub zainfekowana? Zespoły InfoSec mogą wyszukiwać indywidualne wskaźniki ataku (IOA) i wskaźniki naruszenia bezpieczeństwa (IOC) w całej organizacji w celu znalezienia narażonych maszyn, które mogą nie generować żadnych zewnętrznych oznak naruszenia ani dla użytkowników, ani dla administratorów bezpieczeństwa.

Pełna wizualizacja ataku z analizą przyczynowo-skutkową

Sekwencje zdarzeń krok po kroku od początkowego wektora ataku pocztą elektroniczną do infekcji pierwszego klienta, eskalacji przywilejów, rozpoznania środowiska, przemieszczania się po zasobach, gromadzenia danych i eksfiltracji.

Zapobiegaj ponownemu wystąpieniu ataku

Przeanalizuj drogi jakimi przebiegały skuteczne (i częściowo skuteczne) ataki i określ sposoby eliminacji tych luk i punktów dostępu w przyszłości dla powtarzających się ataków tego samego lub podobnego rodzaju.

Triage i priorytetyzacja alarmów za pomocą jednego kliknięcia

EDR pomaga zespołom InfoSec w szybkiej identyfikacji i priorytetyzacji incydentów celem zwrócenia na nie szczególnej uwagi i podjęcia działań zaradczych. Często za pomocą jednego kliknięcia można zakończyć działanie podejrzanych procesów, poddać kwarantannie szkodliwe pliki, dodać atakujące domeny do czarnej listy itp.

Zmniejsz obciążenia operacyjne

Bitdefender EDR zmniejsza obciążenie operacyjne dla naszych klientów dzięki funkcjonalnościom, które są szybkie i łatwe do wdrożenia, nie wymagają specjalistycznych umiejętności do ich obsługi i zużywają minimalną ilość zasobów systemowych. Produkt jest elastyczny, skalowalny i możliwy do rozbudowy do pełnej platformy ochrony punktów końcowych a także wspiera zarządzane usługi bezpieczeństwa jak Bitdefender MDR.

Zlikwiduj lukę kompetencyjną w zakresie cyberbezpieczeństwa.

Pomaga organizacjom średniej wielkości zniwelować luki kompetencyjne w zakresie cyberbezpieczeństwa, dzięki łatwym w obsłudze, wbudowanym schematom postępowania, które umożliwiają skuteczne reagowanie na zagrożenia w celu powstrzymania trwających ataków i usunięcia powstałych szkód. Wizualizacje zagrożeń ukierunkowują dochodzenie pozwalając zrozumieć złożone detekcje, zidentyfikować pierwotne przyczyny ataków i umożliwiają klientowi jak najszybszą reakcję.

Zarządzaj i ograniczaj ryzyko organizacyjne

Technologia Bitdefender EDR pomaga również klientom ocenić i zminimalizować ich całkowite ryzyko organizacyjne — szczególnie w obszarach błędnej konfiguracji systemu, podatności aplikacji i ryzyka ludzkiego - pokazując zespołom InfoSec dokładnie, gdzie pojawia się ryzyko i priorytetyzując zadania niezbędne do szybkiego złagodzenia danego ryzyka.

Narzędzia EDR vs. SIEM

EDR zoptymalizowany dla średniej wielkości zespołów ds. bezpieczeństwa

EDR stanowi "płaszczyznę pośrednią" pomiędzy ochroną punktów końcowych a kompleksowym systemem zarządzania informacjami i zdarzeniami bezpieczeństwa (SIEM). Narzędzia SIEM są rozbudowane i pełnią cenną rolę w większych przedsiębiorstwach. Są one jednak drogie — początkowo w zakupie, a na bieżąco pod względem kadrowym, operacyjnym i eksploatacyjnym - co sprawia, że są one poza zasięgiem małych i średnich przedsiębiorstw i nie są odpowiednie dla małych i średnich przedsiębiorstw.

Systemy SIEM zazwyczaj koncentrują się na określonych typach alarmów, pojedynczych zdarzeniach lub wskaźnikach — nie są zaprojektowane do kompleksowej obsługi incydentów, ataków lub kampanii, a także związków przyczynowych, przebiegu lub powiązań między zdarzeniami. Pozostawia to wykwalifikowanym analitykom możliwość wyciągnięcia własnych wniosków na temat tego, co dokładnie zawierają dane. Wizualizacje danych, które sugerowałyby zależności między incydentami, muszą być opracowywane samodzielnie, co prowadzi do znacznego zróżnicowania wyników w poszczególnych zespołach.

Systemy SIEM nie dają możliwości podejmowania działań. Agregują one wyniki jednokierunkowych przepływów danych bez możliwości odwołania się do systemów, z których pochodzą. Nie umożliwiają dokonywania aktualizacji, ani podejmowania bezpośrednich działań naprawczych z poziomu narzędzia SIEM. Nowe zdarzenia są po prostu zapisywane obok wcześniejszych. W rezultacie wykwalifikowani analitycy otrzymują mnóstwo informacji wyjściowych, które mogą przeszukiwać, korelować i wyciągać własne wnioski — w zależności od swoich umiejętności i doświadczenia.

EDR jest zaprojektowany pod kątem wykrywania i reagowania na incydenty. Automatycznie podnosi poziom pojedynczych alarmów do rangi kompleksowych incydentów, pokazując łańcuch przyczynowo-skutkowy na wszystkich etapach ataku. Dzięki temu możliwe jest natychmiastowe podjęcie działań śledczych i naprawczych bezpośrednio z poziomu konsoli. Ponadto, EDR jest "dla każdego", ponieważ ułatwia wykrywanie i reagowanie małym, średnio wykwalifikowanym zespołom InfoSec.

EDR (Endpoint Detection and Response)	SIEM (Security Information & Event Management)
Zaprojektowany do monitorowania incydentów bezpieczeństwa punktów końcowych	Agreguje ogólne zdarzenia i logi bezpieczeństwa
Dwukierunkowy przepływ danych do systemów źródłowych	Jednokierunkowy przepływ danych tylko z systemu źródłowego
Gotowe pulpity reagowania na zagrożenia	Analitycy muszą tworzyć własne pulpity.
Czytelne wizualizacje łańcucha przyczynowo-skutkowego ataku	Brak wbudowanych wizualizacji łańcucha ataku
Automatyczna analiza i priorytetyzacja incydentów	Stopień zagrożenia jest określany przez analityka
Schematy postępowania i zalecenia dotyczące reagowania na zagrożenia	Analityk określa kroki i kolejność reakcji
Umożliwia bezpośrednie działania osobom odpowiedzialnym za bezpieczeństwo	Nieprzydatne dla osób reagujących na zagrożenia
Zoptymalizowane dla specjalistów ds. bezpieczeństwa w mniejszych zespołach	Przeznaczone dla specjalistów ds. bezpieczeństwa w dużych zespołach

Tabela 1: Porównanie narzędzi EDR i SIEM

Dlaczego EDR to lepsze rozwiązanie

EDR jest oczywistym wyborem dla skutecznego wykrywania i reagowania na zagrożenia przez specjalistów ds. bezpieczeństwa w średniej wielkości zespołach InfoSec w małych i średnich przedsiębiorstwach. SIEM natomiast utrzymuje przewagę w zakresie analizy "big data" i korelacji alertów z wielu źródeł dla dużych zespołów wysoko wykwalifikowanych specjalistów ds. bezpieczeństwa.

- EDR jest zaprojektowany w oparciu o incydenty, a nie alerty, dzięki czemu powiązane zdarzenia są uporządkowane tworząc całościowy obraz
- EDR zawiera gotowe, łatwe do wykorzystania pulpity nawigacyjne ułatwiające szybką reakcję na incydenty
- Osoby reagujące na incydenty mogą podejmować bezpośrednie działania naprawcze wprost z poziomu konsoli EDR
- Analitycy mogą analizować wyniki zapytań i powiązania pomiędzy IOC i IOA w całym przedsiębiorstwie
- Zespoły zajmujące się bezpieczeństwem mogą przeprowadzać analizy przyczyn źródłowych przy użyciu czytelnych wizualizacji łańcucha ataków
- Administratorzy mogą oszacować i zredukować ryzyko systemowe w systemach operacyjnych punktów końcowych, aplikacjach i w odniesieniu do zasobów ludzkich
- Osoby odpowiedzialne za reagowanie na incydenty mogą szybko oceniać i nadawać priorytety alertom, a następnie postępować zgodnie z przejrzystymi instrukcjami naprawczymi"

Wykraczając poza EDR

Ochrona punktów końcowych jest niezbędna do zapewnienia zgodności z normami oraz do odpierania mało skutecznych tradycyjnych ataków, jednak ma swoje ograniczenia. Endpoint Detection and Response jest znacznie lepiej przystosowany do radzenia sobie z zaawansowanymi, wieloetapowymi i wielowektorowymi atakami, które są zaplanowane tak, aby omijać systemy pierwszej linii obrony.

Rozwiązanie **Managed Detection and Response (MDR)**, przeznaczone dla menedżerów przedsiębiorstw zorientowanych na wyniki w zakresie bezpieczeństwa, a nie na narzędzia, zapewnia maksymalne wykorzystanie możliwości pakietu bezpieczeństwa dzięki optymalnej analizie i reakcji wykwalifikowanych ekspertów ds. bezpieczeństwa pracujących przez całą dobę w wyspecjalizowanym **Centrum Operacji Bezpieczeństwa** (ang. Security Operations Center – SOC).

Co niesie przyszłość?

Network Detection and Response (NDR) przenosi EDR na wyższy poziom, wykorzystując analizę ruchu sieciowego generowanego przez tradycyjne punkty końcowe, jak również urządzenia IoT, w celu stworzenia kompleksowego obrazu aktualnego środowiska zagrożeń. Ponadto funkcja rozszerzonego wykrywania i reagowania (XDR) automatycznie gromadzi i koreluje dane z wielu obszarów kontroli bezpieczeństwa przedsiębiorstwa - poczty elektronicznej, punktów końcowych, serwerów, systemów chmurowych i sieci - dzięki czemu zagrożenia mogą być szybciej wykrywane, a analitycy bezpieczeństwa mogą skrócić czas dochodzenia i reakcji we wszystkich obszarach bezpieczeństwa. To ujednolicone podejście do bezpieczeństwa zapewnia pełną widoczność modeli danych i zdarzeń w sieciach, chmurach, punktach końcowych i aplikacjach, jednocześnie wykorzystując analitykę i automatyzację do wykrywania, analizowania, tropienia i usuwania zaawansowanych zagrożeń w całym przedsiębiorstwie. W tym kierunku zmierza przyszłość portfolio bezpieczeństwa Bitdefender.

O Bitdefender

Zwycięska ochrona punktów końcowych

Bitdefender konsekwentnie zajmuje czołowe miejsca w testach i badaniach przeprowadzanych przez niezależne organizacje:

- Pierwsze miejsce w rankingu PC Mag Editors Choice w kategorii "Best Hosted Endpoint Protection and Security Software for 2020"
- "Największy dostawca usług EDR, którego nie brałeś pod uwagę, choć powinieneś" - Forrester Wave w kategorii EDR 2020
- Ocena skuteczności wykrywania MITRE ATT&CK 2020 - Bitdefender wyróżniającym się dostawcą rozwiązań EDR dla średnich organizacji i MSP
- 100% wykrytych zagrożeń w testach „real-world" - GravityZone Ultra EDR w testach AV-Test, styczeń--październik 2020 r."

Zobacz jak działa Bitdefender EDR

- Obejrzyj video poświęcone EDR:

- Część 1: Zaawansowane zagrożenia i zastosowania
- Część 2: Omówienie techniczne i prezentacja produktu

• Uzyskaj darmową 1-miesięczną wersję próbną Bitdefender Endpoint Detection and Response w ramach naszej wyjątkowej, ograniczonej czasowo oferty

• Dostawcy usług, otrzymają darmową 45-dniową, pełną wielodostępową wersję próbną Bitdefender GravityZone Cloud MSP Security

Dowiedz się więcej i zobacz prezentację

Skontaktuj się z nami, aby zarezerwować termin szczegółowej prezentacji produktu i omówienia rozwiązania Bitdefender Endpoint Detection and Response w wersji standalone lub GravityZone Ultra dla EPP+EDR. Dowiesz się, jak rozwiązania te współgrają ze sobą w celu zapobiegania i wykrywania zaawansowanych ataków oraz zapewnienia szybkiej eliminacji zagrożeń.