profinit.
NEW FRONTIER GROUP

Specifika bankovního prostředí při monitoringu a analýze bezpečnostních incidentů

RNDr. Ondřej Zýka
Profinit

IT řešení, které přináší ovoce

Obsah

- Popis situace
- Architektura systému
- Specifika bankovního sektoru
- Praktický příklad – Přínosy a řešení

profinit.
NEW FRONTIER GROUP

New Frontier Holding

1200 zaměstnanců / 2.5 miliardy Kč

profinit.
NEW FRONTIER GROUP

Popis situace

profinit.
NEW FRONTIER GROUP

Rozsah problému

- Údaje z USA za rok 2004
- „Normální“ krádeže, bytová vloupání a ukradená auta a loupeže
  - 16 miliard dolarů
- Nepřiznané daně podle Internal Revenue Service (finanční úřad)
  - 350 miliard dolarů
- Krádeže a podvody ze strany zaměstnanců
  - 600 miliard dolarů

profinit.
NEW FRONTIER GROUP

Co ovlivňuje podvádění

- Dan Ariely – profesor ekonomie na MIT
  - Pokusy se studenty na Harvard Business School a MIT
- Závěry
  - Pokud je příležitost podvádět, tak lidé podvádějí
  - !!! Velikost podvádění není závislá na pravděpodobnosti odhalení
    - Možnost zničit důkazy nezvětšuje mírů podvádění

profinit.
NEW FRONTIER GROUP

Co ovlivňuje podvádění

- Závěry
  - Ochota podvádět je dána okamžitým morálním rozpoložením
  - Účinkuje
    - Odkaz na morální kodex
    - „Tento experiment se řídí etickým kodexem MIT“

- Dan Ariely: Predictably Irrational, HaperCollins, 2008

Současný stav

- Analýza KPMG
  - 348 případů vyšetřovaných v 69 zemích světa
- „Typický" podvodník
  - je muž
  - ve věku mezi 36 a 45 lety,
  - který pracuje ve funkci finančního manažera a/nebo s financemi spojené roli a
  - je ve společnosti více než 10 let na vyšší manažerské pozici.
  - Nepracuje sám - v 61% zkoumaných případů se podvodník domluvil s interní nebo externí třetí stranou.

profinit.
NEW FRONTIER GROUP

Současný stav

- Mnoho podvodů bylo odhaleno formálním nebo neformálním "ohlášením" nebo obdobnými "mechanismy". Spolu s náhodným objevem podvodu, byly tyto metody zodpovědné za objev téměř poloviny všech odhalených případů.

- Jen 6 procent z případů podvodů (v roce 2011) bylo primárně odhaleno na základě varování nebo systémové kontroly. Ve srovnání s 24 procenty v roce 2007 došlo k podstatnému poklesu.

profinit.
NEW FRONTIER GROUP

Současný stav

- Celosvětově
  - Pouze 23 procent odhalených případů bylo veřejně oznámeno.
  - Pouze 46 procent bylo sděleno alespoň interně.
- Východní Evropa
  - Pouze 11 procent bylo hlášeno externě.
  - Méně než 30 procent z podvodu nahlášeno interně.

profinit.
NEW FRONTIER GROUP

Současný stav

- Protikorupční opatření se rozšiřují (i ve státní správě).
  - Nemají odpovídající vliv na zaměstnance a jejich vnímání neetické chování managementu.
  - Většina zaměstnanců věří, že neetické jednání je tolerován více než kdy jindy.
- Asi 54 procent českých manažerů a členů správních a dozorčích rad bylo ochotno dělat etické kompromisy, aby dosáhli finančních cílů svých společností.
- Pouze 18 procent respondentů v manažerských pozicích (striktně) odmítlo neetické chování jako prostředek k dosažení firemních finančních cílů.
- Třetina dotázaných českých respondentů z exekutivy nevěřila, že se vedení chová čestně a eticky.

profinit.
NEW FRONTIER GROUP

Specifika bankovního sektoru

profinit.
NEW FRONTIER GROUP

Legislativní rámec

- Zákon č. 124/2002 Sb., o převodech peněžních prostředků, elektronických platebních prostředcích a platebních systémech (zákon o platebním styku)

- Opatření České národní banky č. 3 ze dne 25 května 2006
  - Toto opatření zapracovává příslušné předpisy Evropských společenství a stanoví požadavky na vnitřní řídicí a kontrolní systém instituce elektronických peněz včetně požadavků na vnitřní audit a řízení rizik.

- Opatření České národní banky č. 1 ze dne 8. září 2003
  - K vnitřnímu řídícímu a kontrolnímu systému banky pro oblast předcházení legalizace výnosů z trestné činnosti

profinit.
NEW FRONTIER GROUP

Profesní rámec

- **Association of Certified Fraud Examiners** (ACFE)
  - Založena 1988 se sídlem v Austinu
  - Funguje i pobočka v České republice
  - Sdružuje, vzdělává a certifikuje vyšetřovatele podvodů
  - Vydává knihy - Fraud Examiners Manual - International Edition

profinit.
NEW FRONTIER GROUP

Specifika bankovního sektoru

- Nutnost vyhovění regulátorům a držitelům standardů
  - Česká národní banka
  - VISA, MasterCard, …
  - SWIFT
- Rozvinuté IT
  - mnoho systémů (produkčních i dohledových),
  - mnoho technologií,
  - mnoho správců,
  - složitá governance.

profinit.
NEW FRONTIER GROUP

Architektura systému pro analýzu a monitoring bezpečnostních incidentů

profinit.
NEW FRONTIER GROUP

Uživatelská pravidla
Komplexní algoritmy
Umělá inteligence

On-line události
Batch zpracování

Realtime akce
Realtime hlášení
Adhoc analýzy
Reporting

Unifikace
Historie
Scoring
Externí zdroje

profinit.
NEW FRONTIER GROUP

Praktický příklad

Přínosy a řešení

profinit.
NEW FRONTIER GROUP

Security datastore

- Implementace řešení v bankovním sektoru
- Nasazení
  - Integrace osmi produkčních systémů
  - Pět měsíců
  - 3TB dat
- Další rozvoj v rámci údržby
  - Přidávání dalších systémů
  - Zvýšení počtu sledovaných vzorců chování

profinit.
NEW FRONTIER GROUP

Požadavky

- Údržba
  - Jednoduchá konfigurace parametrů a pravidel
  - Relativně snadné rozšíření o další vzorce defektního chování (scénáře)
  - Snadné rozšíření o nové zdroje dat
- Systém doplňuje a komunikuje s ostatní dohledovými systémy
- Součástí řešení je i metodika pro upravování stávajících a vývoj nových vzorců chování
- Schopnost implementovat složité algoritmy obsahující parametry, black listy a white listy.

profinit.
NEW FRONTIER GROUP

Přínosy

- Unifikace všechny (bezpečnostních) událostí
  - Systém obsahuje katalog událostí
    - popis,
    - zdrojový systém,
    - identifikací ve zdrojovém systému,
    - různé kategorizace událostí.
- Systém integruje (bezpečnostní) události z více systémů
  - Systém pro retail zákazníky
  - Systém pro korporátní zákazníky
  - Systém pro správu majetkových účtů
  - CRM
  - Náhledy na podpisové vzory
  - Audit databází
  - Datový sklad
  - Internetové bankovnictví
  - . . .

profinit.
NEW FRONTIER GROUP

Přínosy

- Snížení nutnosti detailní znalosti jednotlivých systémů analytiky
- Zjednodušení a zkrácení analýz
- Schopnost analyzovat kompletní historii
  - Možnost opakovaného výpočtu scénářů s upravenými parametry
  - Možnost výpočtu nových scénářů nad historickými daty
- Eliminace různých dob uchovávání logů v jednotlivých systémech

profinit.
NEW FRONTIER GROUP

Specifika bankovního sektoru

- Nedostatečná identifikace událostí
  - Časová – banka pracuje s denní granularitou
  - Místní
    - Potřeba IP adresa,
    - Organizační struktura,
    - Geografická lokace.
- Nedostatečná integrace mezi systémy
  - Nutnost pokrýt celý obchodní proces

profinit.
NEW FRONTIER GROUP

Specifika bankovního sektoru

- Sledován i pouhý náhled na informace
  - Podpisové vzory,
  - Stavy účtů,
  - Obchodní operace.
- Sledována vazba mezi interními zaměstnanci a zákazníky
- Datový sklad nemůže být úložiště bezpečnostních informací

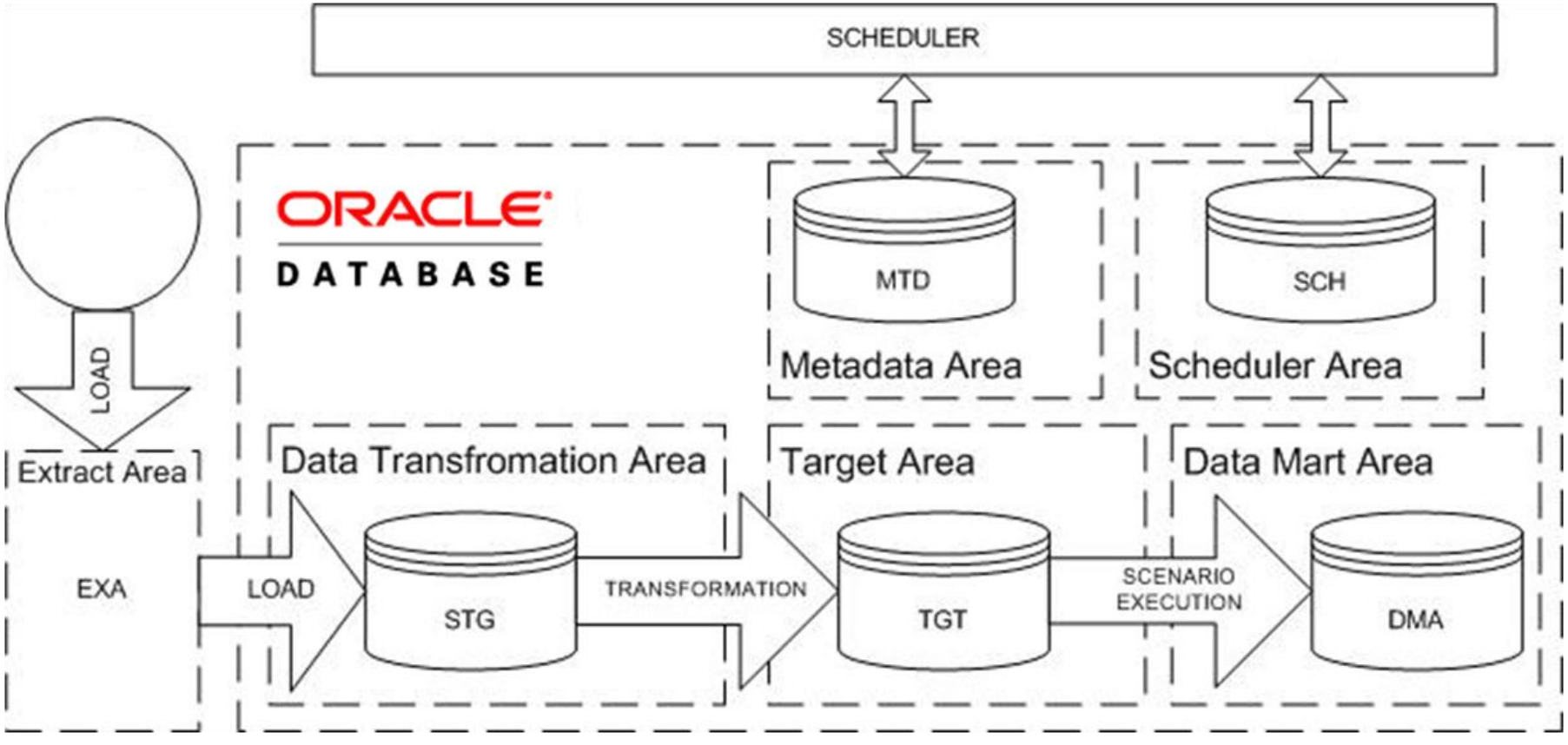
profinit.
NEW FRONTIER GROUP

Základní princip řešení

- Vytvoření specializovaného datového úložiště
  - Mimo datový sklad
  - Zvýšená bezpečnost
- Definice scénářů jako popis defektního nebo podezřelého chování.

profinit.
NEW FRONTIER GROUP

Architektura



Databáze: Oracle

Integrace: webové služby, databázový interface, sdílení souborů

Aplikace: Java

profinit.
NEW FRONTIER GROUP

Typy scénářů

- Knihovna desítek potencionálních scénářů
- Obecné scénáře
- Zákaznické scénáře
  - Specifická obchodní pravidla
  - Specifické aplikace
  - Specifické předpisy

profinit.
NEW FRONTIER GROUP

Typy scénářů

- Neoprávněné přístupy
- Změny v nastavení systémů
- Neobvyklé transakce
- Neobvyklé jednání zaměstnance
- Podezřelé vazby mezi osobami
- Geografické kontroly
- Časové kontroly

profinit.
NEW FRONTIER GROUP

Děkuji za pozornost

ondrej.zyka@profinit.eu
pavel.skorepa@profinit.eu

profinit.
NEW FRONTIER GROUP