SBIR Cybersecurity

Projecttitel:	**Een extra zintuig (EEZ)**
Bedrijf:	**Atos**
In samenwerking met:	**SecurityMatters**

Projectsamenvatting

De doelstelling van het project EEZ was drieledig:
1. Het is mogelijk om alle aanvallen op databases (zowel bekende als onbekende) te detecteren met informatie uit het netwerkverkeer.
2. Het is mogelijk om aanvallen op een database te detecteren met een minimaal aantal valse alarmen
3. EEZ creëert bewustzijn over gebruikersactiviteiten op de gemonitorde database.

Het verlies van gevoelige informatie heeft voor veel organisaties een grote impact. Alleen al in 2014 waren meer dan 502 miljoen records met gevoelige informatie buiten organisaties terecht gekomen. De kosten van dataverlies voor organisaties lopen in de miljoenen dollars per jaar. Naast financiële schade veroorzaakt data verlies:
1. schade aan de reputatie van een organisatie;
2. afname van klantvertrouwen;
3. juridische consequenties wanneer het om persoonsgegevens gaat;
4. verlies aan concurrentiekracht wanneer er intellectual property is gestolen.

EEZ beperkt bovengenoemde kosten door dataverlies te detecteren op de meeste gevoelige infrastructuur van een organisatie: de database. EEZ is een database activity monitoring oplossing dat direct in contact staat met de database connectie en maakt het mogelijk om op een gestructureerde manier het netwerkverkeer te observeren (alleen database gerelateerde informatie).

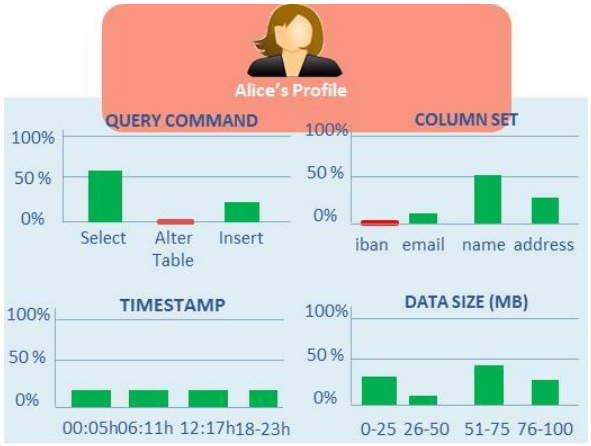
Door het monitoren van iedere transactie op de database, is EEZ in staat met behulp van een geavanceerd model in de software het normale gedrag vast te leggen en elke afwijking hierop als potentiele kwetsbaarheid te signaleren. Uitgebreide testen op online transacties hebben aangetoond dat EEZ de enige oplossing is in zijn soort dat een hoge detectiegraad heeft op zowel onbekende dreigingen als bekende dreigingen tegen lage operationele kosten (de tijd die nodig is om false positives te beheren).

EEZ is een puur op gedrag gebaseerd detectiesysteem: het leert van gebruikersprofielen op basis van een groot aantal kenmerken (zoals SQL queries, data waarden, context informatie). Dit maakt het mogelijk om bekende en onbekende database-aanvallen zonder diepgaande kennis te hebben van potentiële aanvallen.

EEZ is ook een “white-box” oplossing: automatische gegenereerde gebruikersprofielen zijn gemakkelijk te onderzoeken en geven inzicht in het actuele gebruik van de database. EEZ minimaliseert het aantal false positives door het geavanceerde fijnmazige model voor het vastleggen van gebruikersprofielen en door innovatieve feedback mechanismes waardoor het systeem leert van zijn eigen fouten.

Voorbeelden uit reeds uitgevoerde projecten van gedetecteerde dreigingen en misbruik zijn:

- Activiteiten die uitgevoerd zijn op verdachte tijdstippen en locaties (zoals te laat in de avond, te vroeg in de ochtend of op onbekende locaties)
- Toegang tot data buiten de scope van de gebruiker (marketing medewerker kijkt in de data van de financiële administratie zoals iban-gegevens)
- Ongebruikelijke transacties voor een gebruiker (een niet IT specialist voert DLL executies uit, data definition language statements)
- Toegang tot ongebruikelijke hoeveelheden van data (kopiëren van een klantenlijst, ongeacht de tijdsduur die dit kopiëren duurt (uren, dagen))
- Misconfiguratie van gebruikersrechten (te veel rechten voor een bepaalde groep gebruikers)



De belangrijkste voordelen van EEZ zijn:

- Voorziet in een oogopslag inzicht in het gebruik van de database
- Ontdekt verborgen gebruikerspatronen
- Detecteert misconfiguratie
- Detecteert geavanceerde en onbekende dreigingen
- Lage false positive percentage
- Reduceert configuratie en onderhoudskosten
- Geeft direct inzicht in ongeoorloofd data-gebruik

Voor vragen over het product kunt u contact opnemen met Atos via Kees Beeldman (kees.beeldman@atos.net) of via telefoonnummer 088-265 55 55

Deze aanbesteding volgt de Small Business Innovation Research (SBIR) methode. SBIR benut en ontwikkelt kennis, creativiteit en innovatiekracht van het bedrijfsleven voor innovaties die een passend antwoord geven op maatschappelijke opgaven.