Hierodiction Software

EVOTE LGG: Logging- und Auditsystem

EVOTE IDC: Intrusion Detection Cockpit

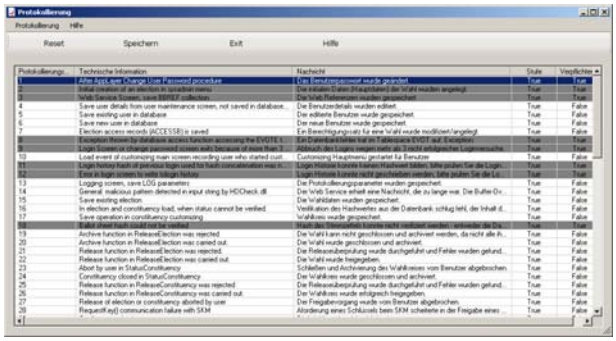
"Logging" vs. Audit System

Konventionelle e-Voting-Systeme oder andere Sicherheitssoftware bietet klassisches Logging, sei es in eine Datei oder in eine (manchmal verschlüsselte) Datenbanktabelle. Dies aber bietet nicht die raschen, real-time Such- und Auditierfunktionalitäten, wie sie in einem e-Voting-System benötigt werden.

EVOTE LGG bietet ein umfassendes Auditsystem, das wie ein Data Warehouse multidimensional strukturiert ist und schnelle, punktgenaue Informationen in einer Auditsituation bietet.

Vorteile

Customisierbarkeit: LGG kann leicht an Ihre Auditerfordernisse angepasst werden, indem es eine große Zahl möglicher Protokollierungspunkte bietet, die aktiviert werden können. Sehr sensible Protokollpunkte sind allerdings immer aktiv.



Verschlüsselung und Datenintegrität: Selbstverständlich sind alle Protokolleinträge verschlüsselt, zusätzlich wird die Integrität aller Einträge durch Hashwerte (SHA-1) gesichert.

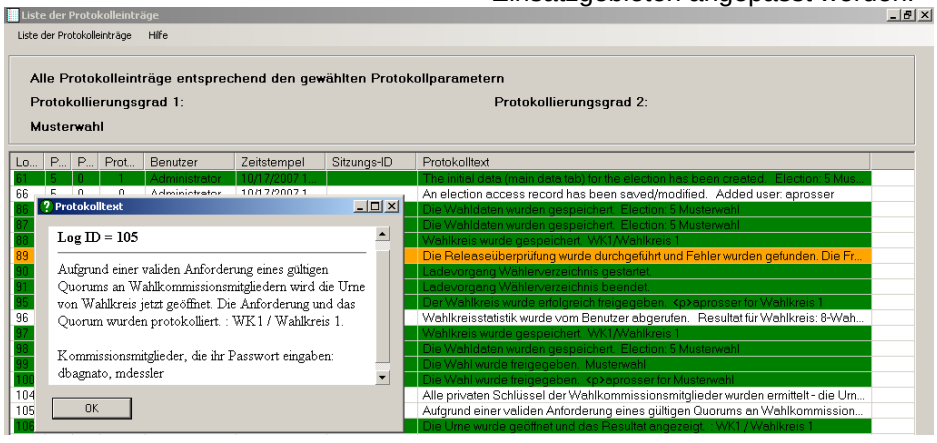
Multi-dimensionale Struktur: Die Protokolleinträge werden in einer multidimensionalen Data Warehouse Struktur gespeichert, die rasche und zielgerichtete Suche ermöglicht, z.B.:

"alle Einträge für einen Wahlkreis", "alle Einträge für einen Wähler", "alle Systemalarme".

Vollständige Nachvollziehbarkeit: EVOTE bietet eine große Zahl von Standardreports über den gesamte Lebenszyklus einer Wahl an. Aufgrund der Flexibilität des Produktes können kundenspezifische Reports definiert werden. Alle Komponenten inkl. VRL und SKM benutzen LGG, wodurch ein umfassender und nahtloser „Audit Trail" sichergestellt ist.

Integration in das Zugriffskonzept: LGG ist nahtlos in das rollenbasierte Zugriffskonzept der jew. Applikation eingebunden und stellt daher sicher, dass nur die Daten eingesehen werden können, für die eine Berechtigung besteht.

Wiederverwendung: LGG ist eine .dll unter .net mit wohldefinierten Schnittstellen und Standardreports, die von anderen Applikationen aufgerufen werden können. Da LGG mit seinem eigenen Tablespace arbeitet, kann es leicht von EVOTE separat in andere Applikationen integriert werden und da einige der Dimensionen im LGG Data Warehouse frei definierbar sind, kann LGG auch leicht an eine breite Palette von Einsatzgebieten angepasst werden.



Kontakt: Hierodiction Software GmbH, Rabengasse 6, A-2230 Gänserndorf. http://www.hierodiction.at

Intrusion Detection Cockpit (IDC)

Das Cockpit ermöglicht es Administratoren EVOTE laufend zu überwachen, v.a. während einer Wahl. Alle Wahlsitzungen werden in LGG vermerkt und jede Anfrage eines Wahlclient wird geprüft:

- ☞ Konsistenz im Prozess,
- ☞ Timeouts,
- ☞ Schadcode

sowie eine große Zahl weiterer verdächtiger Aktivitäten. Auch die Integrität der Daten in EVOTE wird laufend geprüft.

Das Intrusion Detection Cockpit soll Systemadministratoren bei der Betriebsüberwachung unterstützen und jede verdächtige Aktivität erzeugt sofort einen Alarm in der IDC. Auch nicht böswillig herbeigeführte Fehlerzustände im System werden auf diese Weise sofort gemeldet und lenken die Aufmerksamkeit der Systemadministratoren sofort auf den Fehlerzustand. Dabei wird nach folgenden Prinzipien vorgegangen:

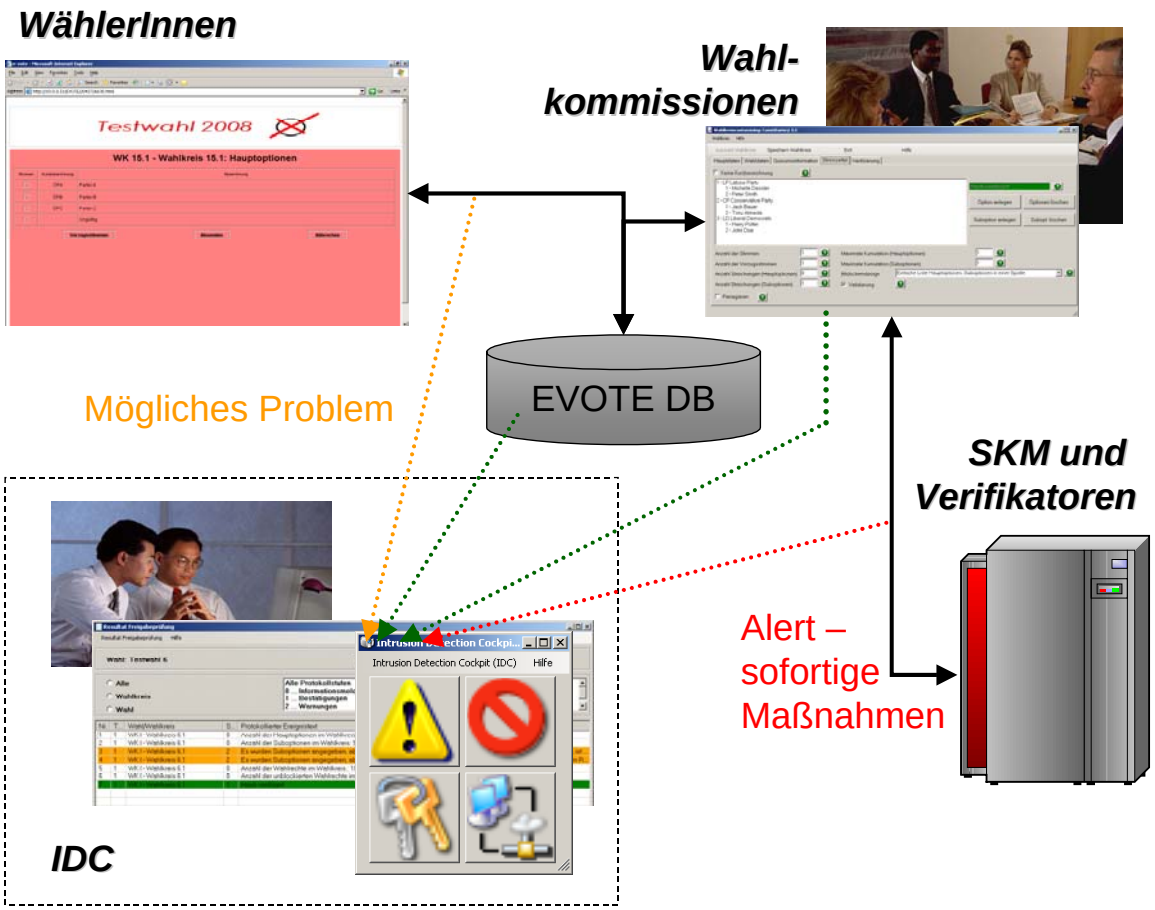
- ☞ laufende Überwachung aller Komponenten,
- ☞ prozessorientierte Überwachung,
- ☞ automatische Bedrohungsklassifikation,
- ☞ Zusatzinformationen zu jedem Alert,
- ☞ sofortige Benachrichtigung der Administration.

Systemaktivitäten werden nicht nur isoliert als solche überwacht, sondern im Prozesszusammenhang gesehen, wobei auch frühere Kommunikationen mit einem Partner berücksichtigt werden. Damit können **auch komplexe Bedrohungsbilder erkannt** werden.

Mit seiner weitgehend **automatisierten Überwachung und Bedrohungsklassifikation** unterstützt die IDC die Systemadministration, die ein „High-Level“ Bild der Systemaktivitäten erhält.

Gleichzeitig jedoch kann zu jedem Alert Detailinformation über Art und Quelle der möglichen Bedrohung angefordert werden, die eine effektive Antwort ermöglichen.

Die IDC deckt alle Komponenten von EVOTE ab und ergänzt so eine infrastrukturelle Intrusion Detection.



Kontakt: Hierodiction Software GmbH, Rabengasse 6, A-2230 Gänserndorf. http://www.hierodiction.at