


Eine neue Epoche für interne Sicherheit – Ihre Daten im Mittelpunkt

Intellinx — Insider Threat Intelligence

Intellinx ist eine neue Dimension von Software für das Monitoring von Unternehmenssoftware, sowohl für die Prävention und die Aufdeckung von Datenmissbrauch, wie auch zur Unterstützung der Innenrevision und des Controllings.



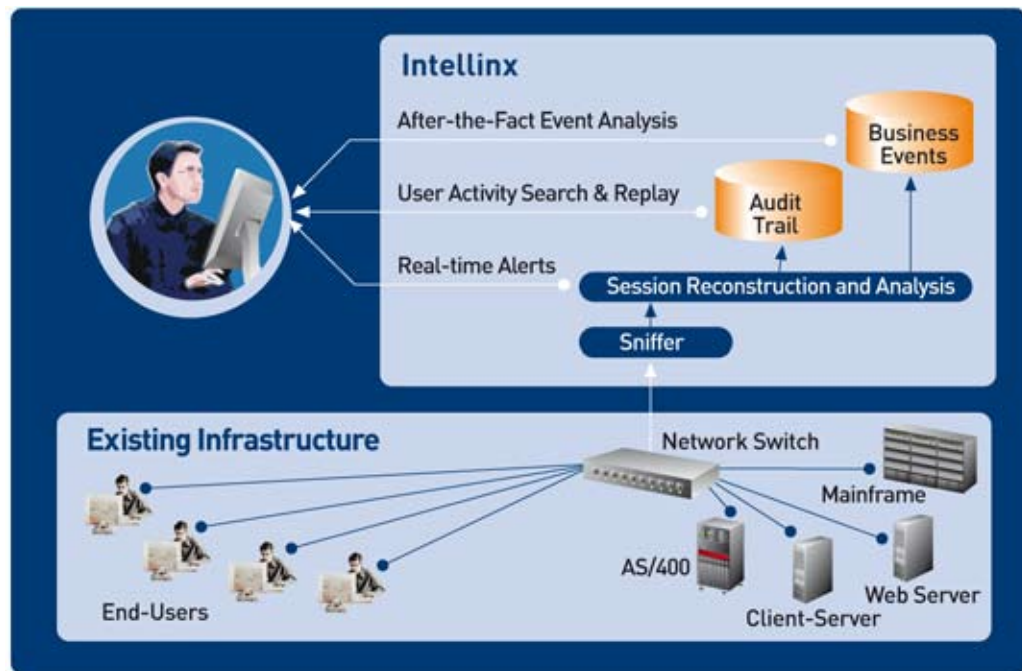
Intellinx arbeitet an der Schnittstelle zum Benutzer und analysiert die Datenströme und spürt Sicherheitslecks beim Gebrauch der IT auf. Herkömmliche Sicherheitssoftware wehrt lediglich Hackerangriffe und unautorisierte Zugriffe von außen ab, nicht jedoch den Datenmissbrauch durch autorisierte Benutzer. Der verursachte Schaden durch autorisierte Benutzer (z.B. Manipulation und Weitergabe von Finanz- und anderen unternehmensinternen Daten) kann zu großen wirtschaftlichen Schäden führen.

Intellinx hilft Bestimmungen wie Sarbanes-Oxley, HIPAA und Basel II umzusetzen. Diese Bestimmungen verlangen unter anderem Interaktionen von Benutzern bis auf Feldebene zu protokollieren. Intellinx benötigt keine zusätzliche Host-Ressourcen, auch sind keine Änderungen an Programmen und Konfigurationen erforderlich.

Bekämpfung von Datenmissbrauch durch autorisierte Benutzer

Eine Hauptsorge in vielen Unternehmen und Organisationen ist das Schützen von kritischen und sensiblen Informationen vor unbefugter Manipulation durch Mitarbeiter. Manipulationen, die vielfach in Straftaten wie Untreue, Bestechung, Insiderhandel, Computerkriminalität, Spionage und Vorteilsannahme, kurz gesagt „Wirtschaftskriminalität“, münden.

Intellinx ist eine neue Dimension für Datenschutzbeauftragte und die Innenrevision und liefert Benutzeraktivitäten in unvergleichbarer Sichtbarkeit. Durch kontinuierliches Aufzeichnen und Analysieren von Benutzeraktivitäten in der Unternehmenssoftware sammelt Intellinx unschätzbares Beweismaterial und verhindert vielfach den Datenmissbrauch. Intellinx ermöglicht ebenso eine visuelle Wiederholung von Bildschirmsequenzen und



Tastatureingaben jeder Anwendung, so als ob über die Schulter des Benutzers geschaut wird. Konfigurierbare Regeln erlauben Verhaltensmuster zu erkennen und einen Alarm in Echtzeit bei Zugriff, durch bestimmte verdächtige Mitarbeiter, auszulösen.

Zum Beispiel kann ein Bankangestellter von Intellinx wahrgenommen werden, der überdurchschnittlich häufig (im Vergleich zu anderen Angestellten) über Kundennamen, nach Kundeninformation in einer bestimmten Stunde oder zu bestimmten Tagen sucht. Intellinx Alarme können ebenso Trigger im Betriebssystem auslösen, zum Beispiel eine automatische Suspendierung eines verdächtigen Benutzers initiieren.

Einhaltung von gesetzlichen Bestimmungen wie Sarbanes-Oxley, Gramm-Leach-Bliley, HIPAA, Basel II

Die Einhaltung von gesetzlichen Bestimmungen stellt eine große Herausforderung dar. Dies gilt besonders für Unternehmen, deren Legacy-Anwendung auf vorhandene, auftragskritische Prozesse abgestimmt ist. Legacy-Anwendungen sind in der Regel vor 10 oder 20 Jahren entwickelt worden und machen es besonders schwierig und aufwendig,

neue gesetzliche Bestimmungen einzu- arbeiten. Das Ergebnis ist häufig ein erhöhtes Betriebsrisiko und Nichterfüllung.

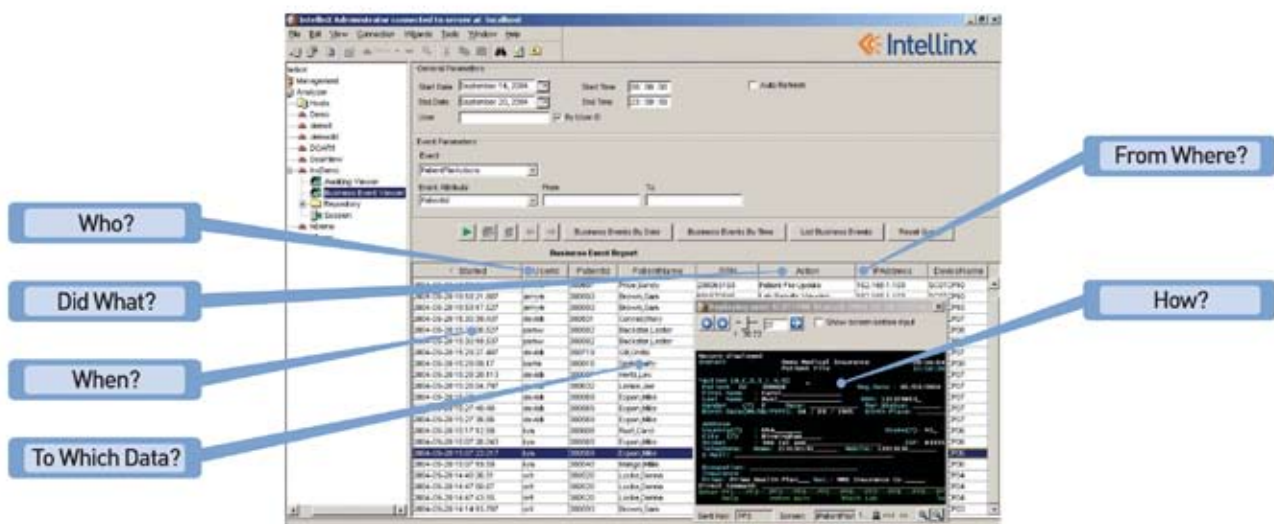
Eine weitere Herausforderung mit denen große Gesellschaften konfrontiert sind, ist die **Einhaltung der Bestimmungen beim Einsatz von heterogenen Plattformen über mehrere Standorte**. Geschäftsprozesse können dabei mehrere Plattformen und Softwaresysteme umspannen. Viele Bestimmungen verlangen ein detailliertes Prüfprotokoll von Benutzerzugriffen auf empfindliche Kundendaten über alle Plattformen. Die Implementierung der gesetzlichen Bestimmungen kann dabei sehr kostspielig sein, da die Änderungen in hunderten oder gar tausenden von Anwendungsprogrammen und die Konsolidierung von vorhandenen Protokollen aus verschiedenen Strukturen und Standorten vorgenommen werden muss.

Erstellen von gerichtsverwertbaren Prüfprotokollen über Benutzeraktivitäten.

Ein detailliertes Prüfprotokoll von Benutzerzugriffen auf sensible, kritische Daten ist eine Notwendigkeit für das Schützen

von korporativen Markenwerten und Informationen. Von Unternehmen und Organisationen verwaltete Zugriffsprotokolle sind häufig aufgrund der folgenden Beschränkungen unzulänglich:

- > Die Protokolle enthalten nicht den Datensatz selbst, bzw. Daten auf Feldebene, sondern lediglich Information auf der Transaktionsebene, d.h. welcher Benutzer griff auf welche Transaktion zu welcher Zeit zu. Wichtig jedoch ist zu protokollieren auf welche Datensätze und Felder der Benutzer zugriff und was wurde durch den Benutzer mit den Daten gemacht.
- > Die meisten vorhandenen Protokolle zeichnen nur Veränderungen auf, nicht jedoch schreibgeschützte Interaktionen. Diese Informationen (wann, wer welche Information sich hat anzeigen lassen) sind ebenso wichtig um einen Datenmissbrauch zu verhindern und dem Vertraulichkeitsschutz den Eigentümern der Informationen gegenüber gerecht zu werden.
- > Die Protokolle stellen eine unvollständige Sicht auf Benutzeraktivitäten dar. Viele Protokolle sind in verschiedenen



Systemen und Anwendungen vorhanden, die es schwierig machen, relevante Informationen zu finden und zu einem Gesamtbild zusammenzufügen.

Legacy-Anwendungen, die über Jahrzehnte entwickelt worden sind, behalten in der Regel keine detaillierten Datenzugriffsprotokolle und sind für solche auch nicht konzipiert worden. Einen Protokollmechanismus in diesen Anwendungen einzuführen bedeutet, jedem Programm Komponenten hinzuzufügen. In großen Unternehmen, die hunderte oder tausende von Programmen im Einsatz haben, ist der Programmieraufwand, um detaillierte Prüfprotokolle in Gänge zu generieren, enorm hoch, häufig sogar exorbitant.

Intellix löst dieses Problem ohne eine Änderung der Programme und ohne die vorhandenen Systeme und Netze zu belasten. Aus den Aufzeichnungen und der Analyse der Benutzeraktivität auf der Anwendungsebene generiert Intellix ein sehr detailliertes Prüfprotokoll von Benutzerzugriffen, Anwendungen und Daten. Es ermöglicht zum Beispiel der Innenrevision, nach all den Benutzern

zu suchen, die auf eine bestimmte Abrechnungsnummer in einem bestimmten Zeitfenster über jede Anwendung und jede Plattform im Unternehmen zugegriffen haben.

Betriebsrisiko (Operational Risk)

Das richtige Einschätzen des Betriebsrisikos wird zu einem wichtigen Aspekt bei einem verlässlichen Risikomanagement. Das Betriebsrisiko ist durch den Basler Ausschuss als „Die Gefahr von Verlusten, die in Folge der Unangemessenheit oder des Versagens von internen Prozessen, Personen und Systemen oder in Folge von externen Ereignissen eintreten“ definiert.

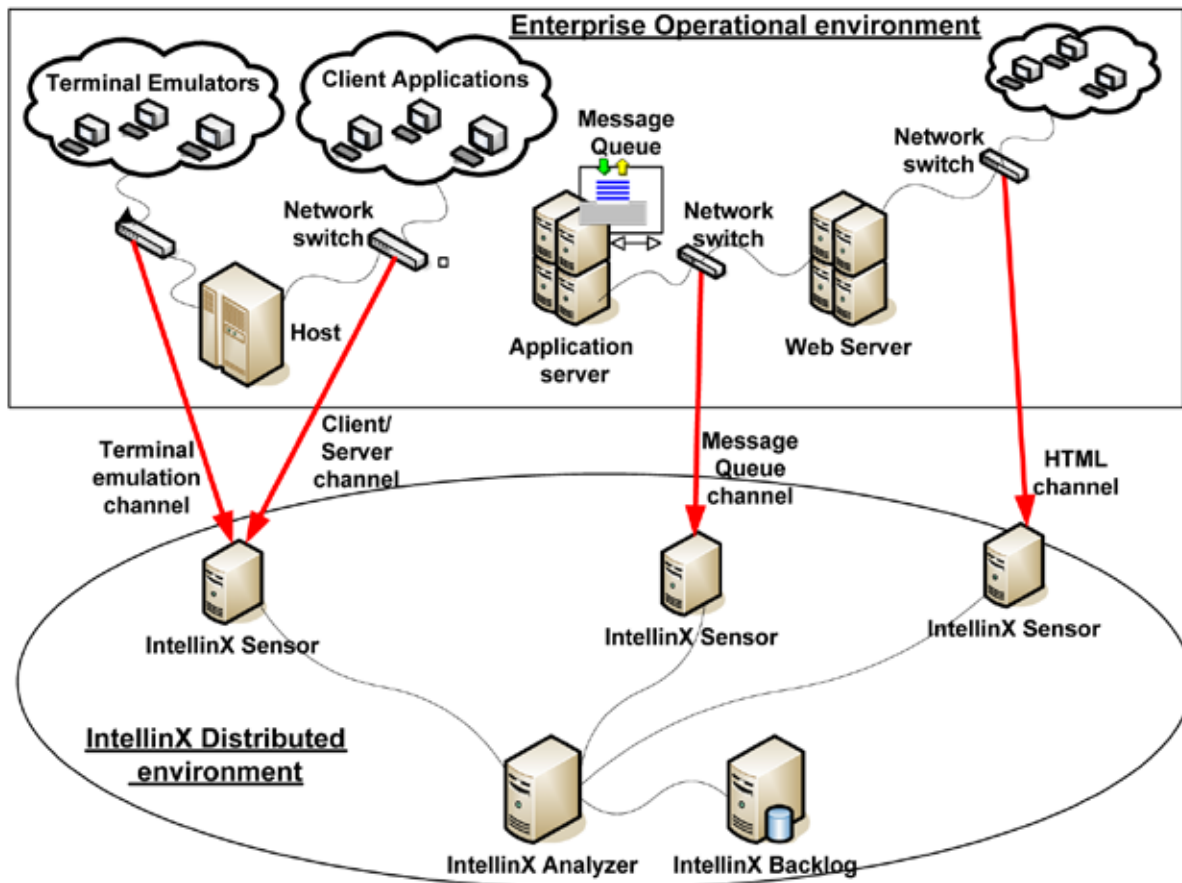
Intellix hilft, interne Prozesse und Interaktionen der Mitarbeiter, die diese Prozesse und die Systeme ausführen, zu überwachen. Regeln können verschiedene Indikatoren bei kritischen Prozessen identifizieren und überwachen und so die Betriebsrisiken in Unternehmen und Organisationen minimieren.

Verfügbarkeit und Leistung

Intellix ermittelt die Verfügbarkeit und die Leistung der Dienste, die von Systeme-

men zu den Benutzern und umgekehrt transportiert werden. Geschäftsprozesse, die aus (auch mehreren) Bildschirmen und Benutzeraktivitäten bestehen, können identifiziert werden und Intellix kann die Antwortzeit und Verfügbarkeit von komplexen Prozessen einschließlich jedes einzelnen Teilprozesses feststellen. Diese detaillierten Informationen sind im Falle einer Leistungsverschlechterung sehr nützlich und helfen, die Stelle im Prozess zu identifizieren, aus dem sich das Problem ergibt.

Intellix unterstützt Service Mitarbeiter des Unternehmens in der Ausübung ihrer Tätigkeit. Service Mitarbeiter können bei einem Benutzer aufgetretene System- oder Programmfehler die Aufzeichnung abspielen und so das Finden des Fehlers deutlich beschleunigen. Zusätzlich kann Intellix nach gleichen Mustern bei anderen Benutzern suchen.



Die Intellinx Architektur ist eine flexible und skalierbare Lösung für Unternehmen und Organisationen mit 100 Mitarbeitern ebenso wie für Gesellschaften mit 100.000 Mitarbeitern. Intellinx unterstützt die folgenden Protokolle:

- IBM Mainframe — 3270 auf Basis von SNA und TCP/IP (TN3270)
- IBM iSeries — 5250 auf Basis von SNA und TCP/IP (TN5250)
- Client/Server — TCP/IP, MQ Series, MSMQ, IBM Mainframe SNA LU0 und LU6.2, SMB
- HTTP

Software AG Österreich
Guglgasse 7-9
1030 Wien, Austria

Tel.: +43 (1)32950-0
Fax: +43 (1)32950-171
www.softwareag.com/austria