# + EGOSECURE FUNKTIONEN

## INTELLACT

Das neue Modul IntellAct analysiert die Fakten, die das Modul Insight ermittelt und löst aufgrund von vorher definierten Regeln Schutzmaßnahmen automatisch aus. Außerdem bietet es die Möglichkeit des Vergleichs mit den Normalwerten, um die Anomalien oder kritischen Situationen automatisch zu erkennen und die entsprechende Schutzreaktion auszulösen. Dieser Automatismus erleichtert die Arbeit der Administratoren enorm und minimiert die Reaktionszeiten deutlich.

## CORPORATE ANALYSIS

### INSIGHT ANALYSIS
Damit die Schutzmaßnahmen optimal eingeführt werden, ermittelt das Modul Insight zunächst die datensicherheitsrelevante Gesamtsituation im Unternehmensnetzwerk. Die Ergebnisse dieser Analyse werden dann managementgerecht aufbereitet und in Grafiken und Tabellen dargestellt. Somit liefert Insight die Fakten, die ein Gesamtbild der Datensicherheit ganz individuell für jedes Unternehmen und jede Organisation zeichnen. Die Darstellung erfolgt kumuliert, so dass Rückschlüsse auf die Tätigkeiten einzelner Benutzer nicht möglich sind. Die Daten in dieser Form sind optimal, um ganz gezielt die Schutzmaßnahmen einzurichten, die wirklich benötigt werden.

### INSIGHT AUDIT
Audit macht die Datenflüsse im Detail sichtbar, zeigt mögliche Schwächen in den Schutzeinstellungen und ermöglicht die Ermittlung forensischer Informationen. Die Möglichkeit, diese Informationen zu generieren ist ein wichtiger Beitrag zur IT-Compliance und entspricht den Vorgaben von Gesetzen und Branchenregularien. Die Datenschutzgrundverordnung (DSGVO) schreibt eine Protokollierung z.B. zwingend vor. EGOSECURE Insight Audit macht gleichzeitig die Verletzung der Persönlichkeitsrechte der Mitarbeiter unmöglich, indem die Einsicht in Protokollierungsdaten durch ein 4 oder 6 Augen Prinzip geschützt wird.

## ACCESS CONTROL

### DEVICE MANAGEMENT
Device Management ermöglicht eine klare Definition, wer welche Devices (z. B. USB Sticks, CDs, TV Tuner) oder Schnittstellen (z. B. WLAN, Firewire, USB) nutzen darf und in welchem Umfang. Somit können alle diese Geräte genutzt werden, ohne dass dadurch Missbrauch oder der Verlust von Daten riskiert wird. Außerdem wird verhindert, dass Malware über die Schnittstellen ins Unternehmensnetzwerk geraten kann. Device Management bietet einen effektiven Schutz gegen „Angreifer von Innen“.

### CLOUD ACCESS CONTROL
Die Nutzung der Cloud hat viele Vorteile in Bezug auf die Flexibilität der Arbeit, da Daten überall zugänglich sein können. Besonders sensible Daten haben jedoch in der Cloud nichts verloren und manche Datentypen dürfen sogar von Rechts wegen nicht auf Cloud-Speichern in sogenannten Drittstaaten gespeichert werden. Cloud Access Control kontrolliert, welcher Mitarbeiter welche Cloud-Dienste in welchem Umfang nutzen darf.

### CONNECTION ACCESS CONTROL
Datenübertragungen sind heutzutage, neben den offiziellen Wegen über das Unternehmensnetzwerk, über viele Wege möglich – Bluetooth, WiFi, Modem, um nur die gängigsten zu nennen. Ein Unternehmen sollte jedoch kontrollieren, über welche Wege Daten das Unternehmen verlassen. Connection Access Control kontrolliert, welcher Mitarbeiter Zugang zu welchen Datenübertragungsgeräten hat.

## FILTER

### CONTENT ANALYSIS & FILTER
Die Analyse von Inhalten und das Filtern von geheimen Informationen aus Daten, die die Firma verlassen, sowie das Blocken von schadhaften Informationen bei eingehenden Daten, sind Bestandteile eines ganzheitlichen Sicherheitskonzeptes. Content Analysis & Filter bietet granularen und zuverlässigen Schutz bei der Datenkommunikation ohne die Arbeitsprozesse und den gewünschten Datentransfer zu behindern.

### ANTIVIRUS
Eine Antivirus-Lösung bietet bewährten Schutz gegen anonyme Angreifer aus dem Internet. EGOSECURE setzt eine Engine ein, deren hohe Erkennungsrate in Testberichten mehrfach bestätigt wurde.

### DATA LOSS PREVENTION
Sensible Informationen, wie Kreditkartennummern, Zugangsdaten oder personenbezogene Daten, aber auch Firmen Know-How, wie Vertragsdaten, Patente oder Konstruktionsdateien , lassen sich leicht in Dokumente kopieren und nach außen tragen. EgoSecure Data Loss Prevention (DLP) prüft den Datentransfer im Unternehmen, anhand von vordefinierten Suchmustern, ob sensible Daten bei der Übertragung vorhanden sind. Wird ein Treffer erzielt, kann die Datei blockiert und somit ein Datenverlust verhindert werden. Außerdem kann der Verstoß protokolliert oder die vertrauliche Datei später verschlüsselt werden. Festplatten können zudem nach sensiblen Daten durchsucht und die Ergebnisse protokolliert werden.

### APPLICATION CONTROL
Application Control kontrolliert, welcher Benutzer welche Programme starten kann. Dadurch wird z. B. vermieden, dass Spiele oder unlizenzierte Softwareprodukte genutzt werden können. Viele Viren können ebenfalls geblockt werden, sogar meist schneller als Antiviren-Lösungen sie erkennen können.

## ENCRYPTION

### REMOVABLE DEVICE ENCRYPTION
Mobile Datenträger, wie z. B. USB-Sticks, werden immer kleiner und leistungsfähiger, wodurch man sie aber auch immer leichter verlieren bzw. stehlen kann. Removable Device Encryption stellt sicher, dass die Daten von Unbefugten nicht genutzt werden können. Die Verschlüsselung findet dateibasiert statt und es sind unterschiedliche Verschlüsselungsarten möglich, die auf einem Medium parallel genutzt werden können.

### FULL DISK ENCRYPTION
Full Disk Encryption bietet umfassenden Schutz für alle Endgeräte durch die komplette Verschlüsselung der Festplatte oder Partitionen auf Sektorenebene. Eine Pre Boot Authentifizierung kann den Benutzer bereits vor dem Start des Betriebssystems authentifizieren. Die automatische Erkennung von neuen Festplatten im integrierten Verschlüsselungschip, blitzschnelle Initialverschlüsselung und ein zentrales Management sorgen für eine reibungslose Integration in bestehende IT-Infrastrukturen.

### PRE BOOT AUTHENTICATION
Pre Boot Authentication sorgt dafür, dass die Anmeldung bei Windows und damit verbundene Verschlüsselungen, wie z. B. die Festplattenverschlüsselung, durch den Umbau der Festplatten, dem Starten von USB/CD oder dem Austausch des Betriebssystems nicht manipuliert und umgangen werden können. Die Anmeldung an das entsprechende Endgerät findet dabei unmittelbar nach dem BIOS-Ladeprozess, jedoch vor dem Start des Betriebssystems, statt. Dabei werden neben Passwörtern auch sehr viele Smart-Cards als Anmeldesicherheit unterstützt. Enterprise-Features wie Help-Desk, Selbstinitialisierung und vieles mehr stehen ebenfalls zur Verfügung. Die Anmeldemasken können an jeweilige Kunden angepasst werden.

### FOLDER ENCRYPTION
Folder Encryption schützt zum einen Daten beim Verlust von Notebooks oder Festplatten, zum anderen aber auch individuell definierte sensible Daten, wenn mehrere Benutzer auf einen Rechner zugreifen können. Sehr geheime Managementdaten können so z. B. auch vor Zugriff von Mitarbeitern mit sehr vielen Rechten geschützt werden.

### CLOUD/NETWORK ENCRYPTION
Mit Cloud und Network Encryption können Ordner in der Cloud oder im internen Netzwerk verschlüsselt werden. Auch bei Auslagerung in die Cloud verbleiben die Verschlüsselungs-Keys im Unternehmen und werden niemals in der Cloud gespeichert.

### PERMANENT ENCRYPTION
Permanent Encryption verschlüsselt Dateien, egal auf welchen Datenträgern sie sich befinden. Diese verschlüsselten Datenpakete bleiben auch bei dem Transfer auf andere Datenwege verschlüsselt. Somit kann durch die Permanent Encryption beispielsweise eine verschlüsselte Datei sicher in einen E-Mail Anhang oder Web-Upload kopiert werden. An fremden Rechnern und Mobile Devices kann die Datei nach Passworteingabe oder durch Nutzung eines PKI-Tokens geöffnet werden.

### ANDROID/IOS ENCRYPTION
Die Verschlüsselung für iOS und Android Devices bietet per App dateibasierten Schutz auf internen Speichern, Speicherkarten und Cloud-Accounts* mobiler Geräte. Die Entschlüsselung findet per Passworteingabe statt.

### MAIL ENCRYPTION
Mit Mail Encryption ist der gesicherte Nachrichtenaustausch möglich, ohne dass auf dem Empfänger oder Sender-PC eine Software-Installation nötig ist. Verschlüsselte und elektronisch signierte Nachrichten lassen sich in gewohnter Umgebung senden und lesen. Auch der verschlüsselte Transport übergroßer Mails kann einfach realisiert werden.

## TOOLS

### MOBILE DEVICE MANAGMENT
Mobile Endgeräte, wie z.B. auch Tablets oder Smartphones, nehmen immer weiter zu. Natürlich müssen sie auch in der Sicherheitsarchitektur berücksichtigt werden. Mobile Device Management sorgt für die intelligente Integration mobiler Endgeräte und unterstützt auch die Betriebssysteme Android und iOS.

### INVENTORY
Zunächst einmal kann man mit Inventory sehen, welche Hardware- und Softwareprodukte auf den Rechnern im Unternehmensnetzwerk installiert sind. Viel wichtiger sind jedoch die Funktionen in Inventory die es erlauben, Veränderungen zu sehen und zu analysieren sowie alarmiert zu werden, wenn sich etwas ändert. Auch der Zustand der Hardware kann angezeigt und so zuverlässig auf Probleme hingewiesen werden.

### PASSWORD MANAGER
Mitarbeiter müssen nicht mehr ihre Passwörter und Logins auf Post-It's oder in Dateien notieren – das übernimmt jetzt der sichere Password Manager. Bereits bei der Erstellung von komplexen Passwörtern kann der Password Manager durch ein intelligentes Verfahren unterstützen. Auch der Austausch von Anmeldeinformationen mit Kollegen wird durch die Ablage der geschützten Password Manager Dateien über das Netzwerk ermöglicht.

### SECURE ERASE
Secure Erase stellt sicher, dass gelöschte Dateien nicht wiederhergestellt werden können, egal ob die Datei sich auf der internen Festplatte oder auf einem externen Speichermedium befindet. Dafür stehen vielfältige Löschmethoden zur Verfügung. Auch bei Verkauf oder bei der endgültigen Ausmusterung von Hardware kann man mit Secure Erase sicher sein, dass man sich wirklich nur von der Hardware trennt.

### GREEN-IT
Intelligentes Powermanagement hilft dabei, die Endgeräte effizient zu betreiben indem nur dann Energie verbraucht wird, wenn der Rechner auch tatsächlich genutzt wird. Green-IT sorgt dafür, dass die Betriebskosten der IT gesenkt werden, die IT einen wichtigen Beitrag zur Umweltbilanz liefert und das für die Einführung von EgoSecure Data Protection ein schneller ROI erreicht wird.

*WebDAV basierte Cloud Dienste (u.a. DropBox, OneDrive, Mediencenter, Yandex & Co.)