

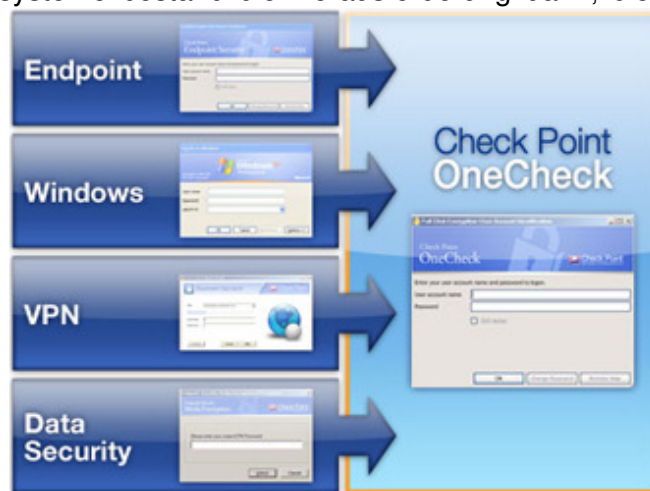
Kundenszenario: Integration von Festplattenverschlüsselung und VPN-Client auf mobilen Endgeräten

Die Anforderungen

Im Versicherungsumfeld ist der mobile Mitarbeiter mit Zugriff auf zentrale Datenbestände bereits seit Jahren der Normalfall. Basierend auf konkreten Schadensfällen und der Veränderung des §42a im Bundesdatenschutzgesetz entstanden jedoch neue Anforderungen im Bereich der Verschlüsselung von mobilen Geräten. Insbesondere die Integration der Verschlüsselungsmechanismen auf Notebooks, PDAs und Smartphones sowie die Ausweitung der Verschlüsselung auf „passive“ Datenträger, wie Festplatten und USB-Sticks wurden hier als zusätzliche Funktionalitäten benötigt. Der Kunde setzt seit Jahren eine 5-stellige Anzahl an VPN-Clients von Check Point zur vollsten Zufriedenheit ein, so dass die Erweiterung dieser Endpoint-Security Komponente nahe liegend erschien.

Die Lösung

Nach Analyse der eingesetzten Geräte und Betriebssysteme bestand die Herausforderung darin, die bestehende Smart-Card-Lösung für Mitarbeiter zu integrieren. Der Login in sämtliche Komponenten sollte durch den einzigen Prozess des Freischaltens einer Smart-Card durch Pineingabe vollzogen werden. Die Unterstützung einer großen Anzahl von Systemen und Smart-Cards der Check Point Lösung stellte hier einen entscheidenden Vorteil dar. Bei der gewählten Lösung handelt es sich um den Check Point Endpoint Security Client. Hiervon werden die Komponenten Endpoint-Connect und Secure-Access für die gesicherte VPN-Anbindung sowie Full-Disk-Encryption für die Boot-Sicherheit und Festplattenverschlüsselung eingesetzt.



Diese Lösung wird sowohl auf Notebooks wie auch auf Window-Mobile basierenden Smartphones verwendet und zentral gemanaged. Dadurch wurde eine Integration der Security-Prozesse zwischen den verschiedenen Geräteklassen erreicht. Darüber hinaus wurden auf den Notebooks die Komponenten Media-Encryption und Port-Protection aktiviert, um den Datenaustausch mit passiven Datenträgern per Policy zu reglementieren. Ziel war hierbei, den Mitarbeitern das Speichern und den Austausch mit derartigen Datenträgern zu erlauben, gleichzeitig aber sicherzustellen, dass kein Dritter die Daten lesen kann. Dies wurde durch eine Policy erreicht, welche ohne aktive Userinteraktion sicherstellt, dass Daten nur verschlüsselt auf derartige Datenträger gespeichert werden können. Andere Mitarbeiter können diese Daten einfach lesen, für Unternehmensfremde sind die Daten unzugänglich. Damit ist eine Sicherung der Daten bei Verlust aller verwendeten Datenträger gewährleistet. Der mögliche Schaden bei Verlust beschränkt sich auf die Hardwarekosten. Damit entstehen keine Berichtspflichten nach §42a bei Verlust von Notebooks, Smartphones, USB-Sticks und Wechselfestplatten.

Zugriff auf sichere Daten aus ungesicherter Umgebung

Die implementierte Lösung bietet bereits sehr guten Schutz der vertraulichen Daten, solange Mitarbeiter von firmeneigenen Geräten aus arbeiten. Gerade im Versicherungsbereich besteht jedoch auch die Anforderung, dass unabhängige Agenten auf die Datenbestände der Versicherungsgesellschaft zugreifen müssen. Dieser Herausforderung erfüllt Check Point mittels eines virtuellen lokalen Desktop, welcher als „sicherer Client im unsicheren Host“ läuft. Hier werden aktuell mögliche Umsetzungsszenarien evaluiert, so dass ein Einsatz dieser Technologie in 2010 für diesen Kunden zu erwarten ist.