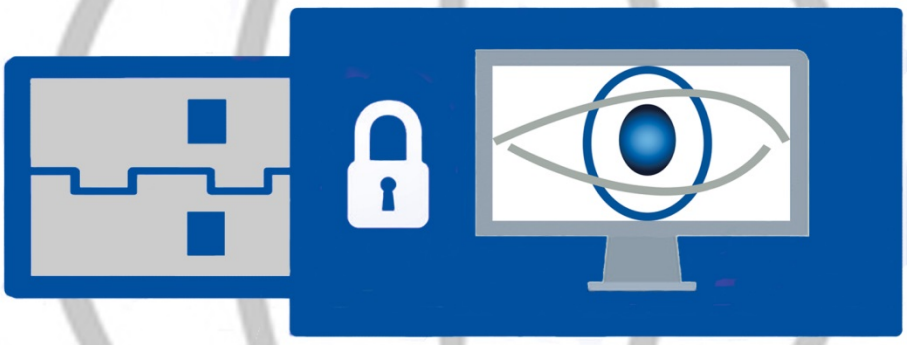
itWESS2Go



Der sichere mobile Arbeitsplatz!

itWatch

itWatch GmbH

Aschauer Str. 30
D-81549 München

Tel.: +49 (0) 8962 03 01 00
Fax: +49 (0) 89 62 03 01 069

www.itWatch.de

itWESS2Go

- Your Secure Portable Workspace

immer und überall einsetzbar, für alle Use Cases

- **am Heimarbeitsplatz**
- **Mobiler Arbeitsplatz unterwegs**
- **Remote Zugang für Fernsteuerung**
- **Automatisierte Fachverfahren mobil**

1. Das Problem

Viele Unternehmen stehen vor dem Problem, wie sie den zunehmenden Wunsch nach Mobilität auch mit einem modernen Konzept abdecken können. Weiterhin sollen sensible Unternehmensdaten verarbeitet werden können, der Zugang von überall ist zu gewährleisten und es gilt so wenig wie möglich „mitnehmen" zu müssen.

Der itWatch mobile Arbeitsplatz kann z.B. in Szenarien wie dem Heimarbeitsplatz, mobilen remote Zugängen zu sensiblen Netzen, Portabilität von besonderen Fachanwendungen, mobile Fernwartungssysteme eingesetzt werden und reduziert die Gesamtkosten signifikant. Der itWatch mobile Arbeitsplatz ist bereits in GEHEIM klassifizierten Netzen im Einsatz und kann in der Auslieferung in verschiedenen Dimensionen beliebig skalieren (Sicherheit, Kosten, Menge, Time to User, etc.).

Letztendlich kann der Kunde seine eigenen Wünsche bezüglich lokalem und zentralem Arbeiten, nutzbarer Anwendungen, automatischer Anpassung der Arbeitsweise an die verfügbare Bandbreite, Vertraulichkeit lokal gelagerter Daten und adäquatem Schutz bei unterschiedlichen Betriebsmodell mit Fokus auf Kosten, einfache Bedienbarkeit und vielen anderen Facetten in dem modularen System einfach umsetzen und so einen sicheren mobilen Arbeitsplatz schaffen, der den eigenen Anforderungen entspricht.

2. Wann ist ein mobiler Arbeitsplatz sicher?

Sensible Informationen verlassen den sicheren mobilen Arbeitsplatz nur über genehmigte vordefinierte Kanäle – dazu zählen Netzwerkverbindungen genauso wie lokale Datenträger oder Ausdrucke auf fremden Druckern. Zu den sensiblen Informationen zählen alle schützenswerten Daten des sicheren mobilen Arbeitsplatzes, insbesondere natürlich Authentisierungsdaten wie Passworte, PINs für Chipkarten etc.

Der Schutz vor Ausspähen ist so organisiert, dass er auch gegen die nicht legale Datenmitnahme und Nachlässigkeiten von den Nutzern der mobilen Systeme schützt. Der sichere mobile Arbeitsplatz wird gleichzeitig vor Infiltrationen von außen geschützt, so dass kein Schadcode nach „innen" gelangt. Der Datenaustausch zwischen dem mobilen Arbeitsplatz und dem Netzwerk wird so reguliert, dass die Datenübergabe ebenfalls nur in berechtigten Kanälen stattfinden kann, verwendete VPN Tunnel also strikt vorgegeben werden können und sogar bestimmte stark authentisierbare Netzwerkkarten mit vordefinierten Verschlüsselungseigenschaften gefordert werden können. Diese sind im Normalfall dann ebenfalls portabel. Datenkopien durch lokale Übergaben können beliebig granular gesteuert werden.

Alle Applikationen am sicheren mobilen Arbeitsplatz werden registriert und authentisiert. Jede sicherheitsrelevante Aktion wird protokolliert. Situationsbewusste Dialoge führen den mobilen Nutzer durch die Besonderheiten seines mobilen Arbeitsplatzes.

3. Was ist der mobile Arbeitsplatz?

Auf einem USB Datenträger (USB-Stick) erhält der Nutzer eine vollständig bootfähige Arbeitsumgebung. Der Stick (mobiler Arbeitsplatz) enthält alle kundenseitig notwendigen Applikationen, Daten und Infrastrukturkomponenten, die zum Arbeiten benötigt werden. Der Stick (mobiler Arbeitsplatz) kann gleichzeitig als Authentisierungsdongle für eine Mehrfaktor-Authentisierung verwendet werden sowie eine SmartCard emulieren und eigenes Kryptomaterial enthalten.

Zusätzlich beinhaltet der Stick eine Sicherheitspolicy, die ein sicheres Arbeiten an einem mobilen Arbeitsplatz z.B. dem Heimrechner ermöglicht. Für den Fall des Heimarbeitsplatzes ist dadurch eine strikte Trennung zwischen Hardware aus eigenem Besitz des Nutzers (oder im Internetcafe genutzte Drittplattformen) und der Hardware, Daten und Infrastruktur des Unternehmens gegeben.

4. Wie ist der mobile Arbeitsplatz geschützt?

Die Sicherheitspolicy bietet nachfolgende Schutzmodule:

- Schutz vor Malware am Datenzugang durch Pattern-Kontrolle mit **itWash**.
- Schutz durch Content-Kontrolle und Pattern-Prüfung mit **XRayWatch.**
- Schutz durch Anwendungskontrolle mit **ApplicationWatch**.
  Durch die Content-spezifischen Rechte der Anwendungen, die auch gegenüber den Benutzerrechten höherwertig sein können, besteht die Möglichkeit zusammen mit der Automatisierung sichere Prozesse abzubilden. in welche der Anwender nicht eingreifen kann.
- Schutz durch Kontrolle der Hardware durch **DeviceWatch**.
- Schutz durch Druckkontrolle mit **PrintWatch**.
- Schutz durch sicheres Löschen von Daten mit **dataEx**.
- Schutz durch sichere Anmeldung am Betriebssystem mit **LogOnWatch**.
- Schutz durch Verschlüsselung vertraulicher Daten mit **PDWatch**.
- Schutz durch revisionssichere Protokollierung aller Vorgänge und Inhalte mit **DEvCon**.

5. Wie wird der mobile Arbeitsplatz betrieben?

Schnelle Bereitstellung, einfache Handhabung und niedrige Betriebskosten zeichnen den mobilen Arbeitsplatz aus.

Gegenüber einem Firmen-PC oder Notebook sehr geringe Investitionskosten.
Die initiale Erstellung eines mobilen Arbeitsplatzes kann an beliebigen Stellen des Unternehmens oder als Managed Service durchgeführt werden. Die Sicherheitsauflagen bei der Erstellung eines mobilen Arbeitsplatzes kann der Kunde aus einem beliebig skalierenden Bereich von Sicherheitsauflagen wählen. Der mobile Arbeitsplatz entsteht dann einfach durch automatisches oder teil-automatisches Aufspielen des Initial-Images auf den Krypto-USB-Stick. Dadurch ist ein einfacher Versand an den Anwender möglich.
Nutzung des mobilen Arbeitsplatzes ist sowohl in der Herstellung als auch in der Verwendung durch technisch wenig versierte Mitarbeiter möglich. Ein kurzes Handout reicht für die Inbetriebnahme. Der Mitarbeiter hat immer seine ihm bekannte Arbeitsumgebung auf einem USB-Stick mit dabei, unabhängig davon an welchem PC oder Notebook er arbeitet.
Durch die zentrale Vor-Konfiguration des USB-Sticks muss der Anwender keine Verbindungsparameter – außer seinen bekannten Zugangsdaten - für den Fernzugriff und die Nutzung der Unternehmensressourcen eingeben. Der Krypto-USB-Stick kann dabei als zusätzlicher Faktor in der Authentisierung herangezogen werden, wodurch bei dem „Remote Login" automatisch eine Mehrfaktor-Authentisierung mit Besitz und Wissen entsteht.
Durch die einfache Herstellung ist der Verlust des mobilen Arbeitsplatzes oder die vollständige Inoperabilität (z.B. nach versehentlichem Reinigen in der Jackentasche) kein Problem, denn durch geeignete SLAs z.B. mit „same day delivery" kann durch einen Logistik Partner die Ausfallzeit auf ein Minimum reduziert werden.
Die tägliche Arbeit bei niedriger Bandbreite am Anschluss des Anwenders wird nicht durch System-Management-Prozesse eingeschränkt – eine Ausnahme können auf Kundenwunsch sicherheitskritische Updates, wie z.B. neue Anti-Viren-Pattern sein. Update- oder Patchprozesse kann der Anwender nach Beendigung der Arbeit oder in der Mittagspause auf Knopfdruck starten. Zentral können maximale Zeiten des
Opt-Out von den System-Management-Prozessen vorgegeben werden.
Bei notwendigen umfangreichen Updates, die – aus welchen Gründen auch immer – nicht über die Netzverbindung gehen sollen, können auch dedizierte
Patch-Stationen in den dezentralen Außenstellen bereitgestellt werden. Der Anwender erhält dann während des Arbeitens die nötigen Informationen, z.B. dass ein größeres Update ansteht und dieses bis in n-Tagen durchzuführen ist. So kann auf beiden Seiten asynchron geplant werden.
Noch komfortabler ist es für den Anwender, wenn bei einem größeren Change
(z.B. Betriebssystemwechsel) der Gesamtprozess auf Logistik abgebildet wird. In diesem Fall erhält jeder Anwender einen neuen Krypto-USB-Stick und wird, wenn er das erste Mal mit diesem bootet, dazu aufgefordert, den alten Stick noch ein letztes Mal einzustecken, so dass zum einen eventuell lokal liegende Daten des Anwenders (Preferences oder Nutzdaten) übernommen werden können und zum anderen nach positiver Datenübertragung der alte Datenträger auch gleich automatisch invalidiert werden kann und für die weitere Nutzung zurück in den Pool gehen kann. Für Sicherheitsrichtlinien und Patches / Updates kann die maximale Zeit der Asynchronizität eingestellt werden und ein Update vor dem nächsten Weiterarbeiten erzwungen werden – dabei kann zwischen lokalem Arbeiten und zentraler Ressourcennutzung unterschieden werden.
Beim Ausscheiden eines Mitarbeiters müssen keine aufwändigen Prozesse durchgeführt werden. Das Invalidieren des Krypto-USB-Sticks kann zentral durchgeführt werden – der Krypto-USB-Stick wird dadurch im Wert auf den Hardware-Wert zurückgesetzt.

6. Systemvoraussetzungen:

- Die Hardware, auf welcher vom Krypto-USB-Stick gebootet wird, muss auf „Booten von USB" umgestellt werden. Eine Maßnahme, die im BIOS der Systeme leicht möglich ist, abhängig vom Wissensstand des Anwenders aber möglicherweise eine Betreuung benötigt. Da zu diesem Systemzeitpunkt keine Remote-Help-Desk Betreuung stattfinden kann, empfiehlt es sich eine optisch verifizierbare „out of band" Kommunikation z.B. über MMS vorab zu vereinbaren.

- Bei der Nutzung von älteren Systemen zum Booten des Krypto-USB-Sticks kann es sein, dass das neue Betriebssystem auf dem Krypto-USB-Stick keine Treiber zu der lokalen Netzwerkkarte kennt. Statt hier den Vorrat an Treibern im Krypto-USB-Stick-Betriebssystem zu erweitern, kann kundenseitig ein Standard-Netzwerkadapter an USB mitgegeben werden, der in diesem Fall verwendet wird. Der Anwender kann nach Inbetriebnahme informiert werden, ob dieser externe Netzwerkadapter nötig ist und – falls nicht – per Dialog informiert werden, dass er diesen externen Netzwerkadapter wieder zurückgeben kann. Dieser Dialog kann zentral protokolliert werden, so dass auch statistische Daten zur Verfügung stehen.