ecos

Notfallarbeitsplätze

Sicherer Zugriff auf die IT-Infrastruktur bei Pandemie, Hochwasser und Streik

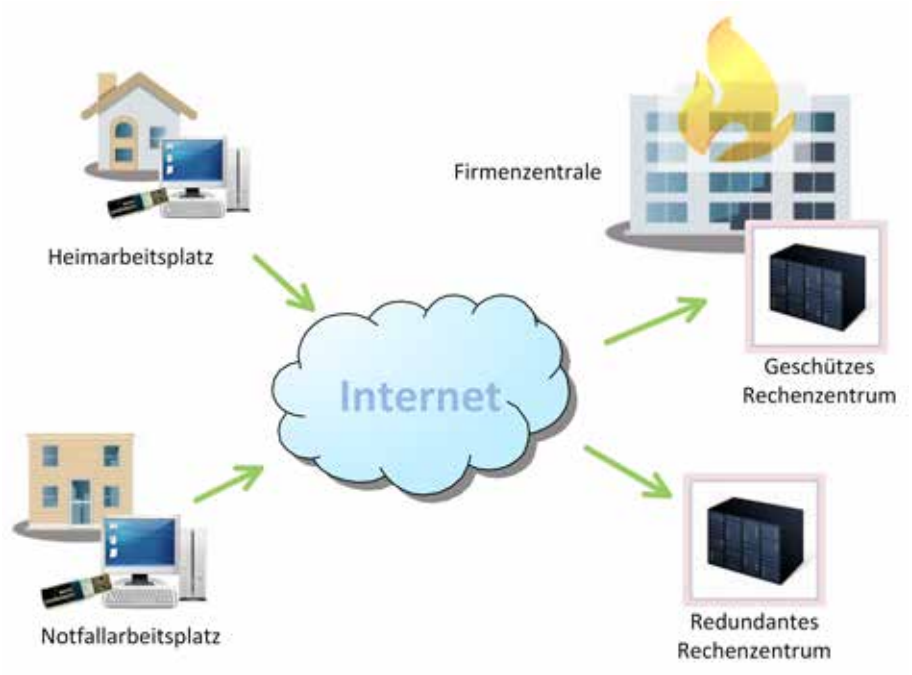
- Risiken vermeiden
- Administration erleichtern
- Beliebige PCs hochsicher einbinden
- Budget schonen

RealStuff Informatik AG

Sicherer Zugriff auf die IT-Infrastruktur im Notfall

Hochwasser, Unwetter, Ausfall der öffentlichen Verkehrsinfrastruktur oder Streik.

Im Notfall ist es erforderlich den Schaden für das Unternehmen durch eine schnelle Wiederaufnahme des Geschäftsbetriebes möglichst gering zu halten. Zu einem umfassenden Notfallplan gehört es daher sicherzustellen, Mitarbeitern ein temporäres Arbeiten von externen Räumlichkeiten oder von Zuhause zu ermöglichen



Beispieldarstellung

Einsatzszenarien

In dem folgenden Szenario wird davon ausgegangen, dass aufgrund einer Katastrophe wie Feuer, Naturkatastrophen, Ausfall der Verkehrsinfrastruktur oder einer Pandemie das Firmengebäude nicht mehr betreten werden kann. Ferner wird davon ausgegangen dass die ITK-Infrastruktur, aufgrund entsprechender Vorkehrungen oder redundanter Systeme, weiter funktionsfähig und erreichbar ist.

Flexible Arbeitsplätze

Gerade in der Verwaltung reduziert sich ein Arbeitsplatz typischerweise auf einen PC und ein Telefon. Werden die entsprechenden Vorkehrungen getroffen, lassen sich alle Tätigkeiten weitgehend von einem beliebigen PC und einem beliebigen Ort aus durchführen. Somit wird eine möglichst rasche Wiederaufnahme des Geschäftsbetriebs im Katastrophenfall sichergestellt.

Notwendige Vorkehrungen

Auf Unternehmensseite ist es notwendig durch eine entsprechende Terminalserver- bzw. VirtualDesktop-Infrastruktur oder Webanwendungen die Basis für einen externen Zugriff auf Daten und Anwendungen zu schaffen.

Anforderungen auf Benutzerseite

Um im Katastrophenfall eine zeitnahe Arbeitswiederaufnahme zu gewährleisten, kann schon allein aus organisatorischen Gründen nur eine installations- und konfigurationsfreie Lösung in Frage kommen. Ferner müssen solche Vorkehrungen höchsten Sicherheitsanforderungen der IT standhalten, um nicht bereits bei normalen Betriebsabläufen zum Sicherheitsrisiko zu werden. Eine starke 2-Faktor Authentisierung ist unerlässlich.

Ein weiterer wichtiger Punkt eine solche Notfallmaßnahme aktuell zu halten. Es muss sichergestellt sein, dass diese bei einem plötzlichen Einsatz nicht hoffnungslos veraltet ist. Im Falle webbasierter Anwendungen ist zudem die Problematik möglicher Browser-Inkompatibilitäten und Erfordernis von Plug-Ins zu beachten.

ECOS MOBILE OFFICE STICK

Flexible Zugangsmöglichkeit

Zur Abdeckung aller Anforderungen auf Benutzerseite, erweist sich der ECOS MOBILE OFFICE STICK als ideale Lösung. Es handelt sich um einen USB-Stick, der von einem beliebigen PC oder Mac genutzt werden kann. Dieser enthält sämtliche Software für den automatischen Aufbau eines sicheren VPN-Tunnels sowie die Verbindung zu Citrix, Microsoft Terminalserver, VMware View oder Webanwendungen. Mit dem ECOS EASY ENROLLMENT wird der Ausgabeprozess so einfach wie möglich gestalten. Hierbei erhält jeder Benutzer einen identisch vorkonfigurierten Stick nebst einem persönlichen Aktivierungscode. Nach Eingabe letzteren und Verifizierung durch die Gegenstelle wird die Sticksoftware aktualisiert und die persönliche Konfiguration geladen und an den Benutzer gekoppelt. Die Lösung ist damit für den Anwender völlig installations- und konfigurationsfrei. Gleichzeitig dient der Stick als zertifikatsbasierte 2-Faktor-Authentisierung (alt. mit Smartcard) und schützt somit vor unautorisierten Zugriffen.

Hardwarelose Lösung

Alternativ zum ECOS MOBILE OFFICE STICK ist auch ein Einsatz des ECOS VIRTUAL WEB CLIENT möglich. Angelehnt an die Funktionsweise des Sticks, werden in diesem Fall die Clients nicht vom USB-Stick geladen, sondern über einen Standard-Browser ad-hoc geladen und völlig installationsfrei ausgeführt. So wäre es auch denkbar von einem IE ausgehend z.B. einen notwendigen Firefox Browser inkl. Plug-Ins zu laden und auszuführen. Als zweiten Faktor kann in diesem Fall eine Authentisierung per SMS-OTP oder beim Rollout ausgegebene OTP-Token erfolgen.

Für höchste Sicherheitsanforderungen

Die zuvor beschriebenen Lösungen schützen gegen mannigfaltige Bedrohungen. Ist es jedoch die Anforderung betriebliche und geschäftliche Nutzung 100% zu trennen, sowie jegliches Ausspähen von Bildschirminhalten durch Trojaner zu verhindern, so empfiehlt sich der ECOS SECURE BOOT STICK. Mit angestecktem Stick, bootet der PC eine speziell gehärtete Linux-Umgebung. Die lokale Festplatte und das darauf installierte Betriebssystem sind deaktiviert, und damit wird eventuell vorhandene Schadsoftware gar nicht erst aktiviert.

Nach erfolgreicher Authentifizierung wird je nach Anforderung ein Citrix-Receiver, RDP- bzw. VMware View Client, oder Browser aufgerufen. Sodann befindet der Anwender sich in der von ihm gewohnten Umgebung. Zur Sicherstellung der telefonischen Erreichbarkeit, ist es möglich, z.B. bei Anbindung des PCs über WLAN, den freien LAN-Port zum Anschluss eines IP-Telefons zu nutzen. Dieses wird über den aufgebauten VPN-Tunnel direkt mit der Telefonanlage im Unternehmen verbunden.

Mit dem ECOS SECURE BOOT STICK, der eine 100%ige Trennung zwischen privater und geschäftlicher Nutzung sicherstellt, wird der Stick zur Firmenhardware und der private Rechner kann quasi als private Peripherie betrachtet werden.

ECOS VIRTUAL WEB CLIENT inkl.SMS-OTP oder OTP Token

ECOS SECURE BOOT STICK

Zentrales User- & Rechtemanagement

Alle ECOS-Zugangskomponenten werden über ein zentrales Benutzer- und Rechtemanagement verwaltet. So lassen sich Zugriffsrechte auch remote aktualisieren oder sogar entziehen, wenn der Benutzer den Stick möglicherweise noch gar nicht aktiviert hat. Im Falle dass ein Stick verloren geht, oder bei einem ausscheidenden Mitarbeiter nicht zurück kommt, kann der Zugang gesperrt und die bestehende Lizenz auf einen neuen Stick übertragen werden

Nicht nur für den Notfall

Natürlich sind die ECOS Zugangslösungen nicht nur im Notfall einsetzbar. Einmal ausgegeben, ermöglichen Sie dringende Angelegenheiten auch z.B. von Zuhause oder vom Hotel aus zu erledigen.

Detaillierte Informationen zu der Funktionsweise der hier vorgestellten ECOS-Lösungen, den umfassenden Sicherheitsmechanismen, dem ECOS EASY ENROLLMENT und der 2-Faktor-Authentisierung liefern unsere Datenblätter und Whitepaper unter:
www.ecos.de

ECOS TECHNOLOGY GMBH
Sant-Ambrogio-Ring 13a
D-55276 Oppenheim

Tel: +49 (6133) 939-200
Fax: +49 (6133) 939-334
info@ecos.de