

Wer kommt da durch die Hintertür?

IT-Support unter Sicherheitsaspekten

Verfasser: Dr. Ulrich Böttger
Informationseigner: Dr. Ulrich Böttger
Klassifizierung: Ka-IT-Si
Stand: 17.11.2011
Version: 1.0

Karlsruher IT-
Sicherheitsinitiative

Agenda

- Beispiele
- Anforderungen
- Aspekte von Fernwartungszugängen
- Desktop-Sharing

Viele Aussagen gelten auch für Support durch eigene Mitarbeiter.

Beispiele für Fernwartungszugänge

- SSH/RDP/VNC/HTTPS
- Desktop od. Applikation über Gateway
- Client-VPN (IPsec, SSL, ...)
- Site-to-Site-VPN
- ISDN-Einwahl
- in the Cloud
- (Desktop-Sharing)

Herausforderungen

- 24x7-Betrieb (Produktion, Handel, Zeitschrift, Verkehrsbetriebe etc.), aber IT nur 9x5
 - ggf. auch zu Zeiten, an denen bei dem Supportnehmer niemand arbeitet
- viele Anbieter, unterschiedliche Systeme/Standorte, teilw. Outtasking
 - ggf. Automatismen (z.B. Backup, Monitoring)
 - Einbindung von Herstellern
 - teilw. keine Einflussmöglichkeit

Angriffsszenarien

- Missbrauch des Fernwartungszugangs durch
 - externen Angreifer
 - ausgeschiedenen Mitarbeiter des Supportgebers
 - aktiven Mitarbeiter des Supportgebers
- Verbreitung von Schadcode über den Fernwartungszugang

Ziele

gemeinsame:

- Beschränkung des Zugriffs auf bestimmte Systeme od. Aktionen
- Information über die zugreifende Person
- Information über die durchgeführten Aktionen
- Verfügbarkeit
- Administrierbarkeit und Skalierbarkeit

Ziele

des Supportnehmers

- Zugriff nur nach vorheriger Freigabe
 - bedeutet Aufwand
 - nicht mit jeder Anforderung vereinbar
- Information, dass ein Zugriff erfolgt

des Supportgebers

- Belegbarkeit des Nicht-Zugriffs

Benutzer-Optionen

- personalisierte Benutzer für jede(n) Support-Mitarbeiter(in) des Supportgebers
 - Nachteil: schlechte Administrierbarkeit
- Role-Account für den Supportgeber
 - Nachteile:
 - keine Unterscheidung der Support-Mitarbeiter
 - Autorisierung schwierig
 - problematisch beim Ausscheiden von Mitarbeitern
- Mittelweg: Role-Account mit personalisierter Authentisierung (z.B. SSH mit Schlüsseln)

Authentisierung

des Supportgebers

- Quell-IP (z.B. durch Firewall-Policy, Site-to-Site-VPN)
- Benutzername/Passwort
 - alleine nicht ausreichend
 - ggf. mehrstufig
- Token, Zertifikate, Schlüssel

des Supportnehmers (z.B. Rückruf, Secret)

- Autorisierung im Vorfeld klären

Supportgeber

- dediziertes Netzwerk
- dedizierte Systeme
- Firewall-Freischaltung (→ Nachvollziehbarkeit, vermeidet Missbrauch und Schadensausbreitung)
- Vorab-Information des Supportnehmers
- Protokollierung
 - auf Firewall
 - Mitschnitt

Supportnehmer

- Application-Level-Gateways (→ Beschränkung des Zugriffs, Verhinderung der Schadensausbreitung)
- Segmentierung, dedizierte Netzwerke für unterstützte Systeme (→ Beschränkung des Zugriffs, Reduzierung der Schadensausbreitung)
- IDS/DLP
- Log/Audit, Übertragung auf abgeschottetes System (→ Nachvollziehbarkeit)

spontaner Support

- Nutzung bestehender Fernwartungszugänge
 - erfordert evtl. die Herausgabe von Passwörtern
- Desktop-Sharing

Nachteile:

- erfordert zumindest teilweise funktionierende Infrastruktur
- Zeitverlust im Störfall

Desktop-Sharing

- Web-basierte Fernwartungs-Tools
 - erfordert Vertrauen in den Anbieter
- Instant Messaging
 - erfordert Vertrauen in den Anbieter
- Fernwartungs-Software mit Gegenstelle beim Supportgeber

Desktop-Sharing (2)

Vorteile:

- Nachvollziehbarkeit
- wenig Vorbereitung beim Supportnehmer

Nachteil: deckt nicht alle Anforderungen ab

- 24x7
- Outtasking
- Firewall-/Webproxy-Support

Zusammenfassung

- individuelle Lösungen
- Fernwartung (besser als spontane Aktion)
 - sicher
 - zielgenau
 - überwacht
- Support setzt Vertrauen voraus, u.a. basierend auf technischem und organisatorischem Know-How.

IT-Betrieb nach Maß

Firmengruppe CONNECT - Wir begeistern!



CONNECT®

Firmengruppe