

Das Internet-Cafe als K-Fall Konzept

Die Bundesanstalt für Finanzdienstleistungsaufsicht (BAFIN) schreibt Finanzinstituten Mindestanforderungen für das Risikomanagement vor, in dessen Rahmen auch ein Notfallkonzept verlangt wird. Die Anforderungen an ein Notfallkonzept sind sehr generisch formuliert und schreiben lediglich vor, dass im Notfall zeitnah Ersatzlösungen zur Verfügung stehen müssen, um den Geschäftsbetrieb aufrecht zu erhalten.

Unser Auftraggeber, ein Finanzinstitut mit 3.500 Mitarbeitern betreibt zur Notfallvorsorge zwei Rechenzentren (kurz RZ), die weiter als 5 km auseinanderliegen und über unabhängige Internet-Zugänge verfügen. Das Back-Up RZ spiegelt alle relevanten Produktions- und Sicherheitssysteme. Ausgehend von einer detaillierten Risikoanalyse, bei der alle Business Owner die Kritikalität ihrer Anwendungen bewerten mussten, wurden ca. 20-30% aller Applikationen als so kritisch eingestuft, das eine Dopplung im Back-Up RZ gerechtfertigt ist.

Das primäre Rechenzentrum des Finanzinstitutes ist im Gebäude des Hauptsitzes angesiedelt, der auch den Großteil der Mitarbeiter beherbergt. Tritt nun der Katastrophenfall – eine komplette Zerstörung des Gebäudes – ein, ist der Betrieb der kritischen Serversysteme durch Übernahme des Back-Up RZs gewährleistet. Der Wegfall der Arbeitsplätze in der Hauptstelle kann nicht durch die Mitarbeiter in den Geschäftsstellen aufgefangen werden, so dass für ca. 400 Mitarbeiter ein Ausweicharbeitsplatz geschaffen werden musste, der innerhalb weniger Stunden zur Verfügung steht.

Das Konzept, das BDG gemeinsam mit dem Auftraggeber entwickelt hat, ist ebenso effektiv wie einfach: Ausgewählten Anwendern wird im Katastrophenfall eine Einwahl- und eingeschränkte Zugriffsmöglichkeit via Terminalserver zur Verfügung gestellt, die mittels starker Authentisierung die echte Identität des Anfragenden prüft. Der Zugriff wird über ein SSL VPN Gateway abgesichert. Die Mitarbeiter benötigen daher im K-Fall lediglich einen PC mit Browser, um den Geschäftsbetrieb aufrecht erhalten zu können. Dieser steht ihnen in der Regel zu Hause oder auch im Internet-Cafe zur Verfügung.

Neben der Umsetzung des K-Fall Konzeptes war zusätzlich eine Strenge Authentisierung für Telearbeitsplätze notwendig, die von ISDN-Einwahl auf VPN-Technologie umgestellt werden sollten.

Nachstehende Projektbeschreibung konzentriert sich auf das Authentisierungskonzept das gewährleistet, dass im K-Fall nicht der Rechner sondern die Person, die Zugriff erlangt, zweifelsfrei identifiziert werden kann.

>>>

Verfasser: Stefanie Alfer

Authentisierungskonzept

Die Anforderungen an das Authentisierungssystem wurden zu Projektstart wie folgt definiert:

Sicherheit

Verschlüsselung beim Datentransfer zwischen Client und Server, Backup und Fallbackmöglichkeit, zertifizierte Technologie basierend auf Standards.

Integrierbarkeit

Die Produkte sollen in die Systemlandschaft des Finanzinstitutes passen; das Verfahren soll die vorhandenen Access-Komponenten, Applikationen und Security-Anwendungen unterstützen.

Flexibilität

Möglichkeit zur Erweiterung durch neue Access Points, weitere Applikationen und zusätzliche Dienste. Z. B. kann auch die Zugangskontrolle in dieses Verfahren einbezogen werden. Verwendung von unterschiedlichen Authentifizierungsdevices: Token, SmartCards, usw.

Zentrale Administration

Einfache und zentrale Verwaltung mit verschiedenen Rollen (Administratoren, User Manager, Help Desk).

Skalierbarkeit

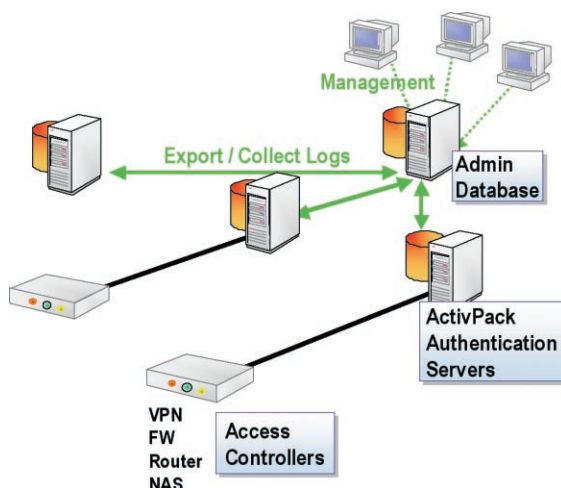
Anpassung an steigende Anforderungen durch zusätzliche User, die Lösung soll erweiterbar sein.

Hochverfügbarkeit

Falls der Authentisierungsserver ausfällt, sollte trotzdem eingewählt werden können. Zur Erhaltung der Hochverfügbarkeit ist ein Backup-Authentisierungsserver installiert.

Unabhängigkeit

Für den Zugriff im K-Fall muss eine Einwahl von Fremd-PCs gewährleistet werden, das System muss ohne Middleware auskommen.



Actividentity™

Ausgewählt wurde die ActivIdentity Lösung, weil sie sowohl SmartCards als auch Token zur Authentisierung unterstützt. Der ActivCard AAA-Server dient zum Management digitaler Identitäten, die Hauptfunktionen sind folgende drei:

- **Authentication: Who are you?**
Prüfung der Identität
- **Authorization: What are your rights?**
Verwaltung der Zugriffsrechte
- **Accounting: What did you do?**
Protokollierung der Aktivitäten

Der AAA-Server von ActivIdentity realisiert eine dreistufige Architektur, die aus einer zentralen administrativen Datenbank, produktiven Authentifizierungsservern und Remote-Managementkonsolen besteht. Änderungen werden von Remote-Managementkonsolen in die zentrale Admin-Datenbank geschrieben und vom Administrator nach Fertigstellung auf die Server exportiert. Umgekehrt werden die Logdaten lokal auf den Authentisierungsservern gespeichert und auf Anforderung in die Admin-Datenbank zur Konsolidierung und Prüfung importiert. Authentifizierungsverfahren lassen sich einteilen auf die Prüfung von drei Faktoren:

- Wissen: PIN, Passwort
- Besitz: Schlüssel, Token, SmartCard
- Merkmal: Aussehen, Biometrie

Durch Hinzufügen einer Authentisierungslösung die aus der Prüfung von zwei der drei Faktoren besteht, wird die Sicherheitsstufe des Verfahrens deutlich erhöht, man spricht von starker Authentifizierung. Bei diesen Methoden wird der Anwender und nicht die Verbindung oder das Gerät authentifiziert, digitale Identitäten werden gemanagt. Diese Zwei-Faktor-Authentifizierung zeichnet sich durch die Kombination von Wissen (PIN) und durch Besitz (Token, SmartCard) aus.

Klassische starke Authentifizierung mit Tokensystemen

Tokenbasierte Systeme arbeiten wie folgt: Der Anwender besitzt PIN und Token und kann sich an vordefinierten Gateways anmelden. Diese Anmeldeagenten müssen für die starke Authentifizierung zusätzlich installiert und konfiguriert werden. Der Anwender erhält seine Zugangsberechtigung durch Bedienung seines Tokens und muss Login und Passwort manuell in ein Anmeldefenster übertragen. Dabei ist keine Software zur Berechnung und Übertragung erforderlich. Dies erlaubt größtmögliche Unabhängigkeit von der Systembeschaffenheit auf Anwenderseite.

>>>

Zur Prüfung der Anfragen ist ein spezieller Authentisierungsserver im Zielsystem erforderlich, eigene Benutzer- / Schlüsselverwaltung ist notwendig, Anbindung an existierende Benutzerstrukturen sind möglich (z. B. durch LDAP an MS Active-Directory, iPlanet und Novell eDirectory), Import und/oder Queryfunktionen werden unterstützt. Die Benutzerverwaltung für den K-Fall und die Telearbeitsplätze erfolgt im Activ Directory des Finanzinstitutes.

Es existieren Hardware-Token verschiedener Ausprägung: Schlüsselanhänger, Karten, Taschenrechner.



Starke Authentifizierung mit SmartCards

Bei Lösungen mit Verwendung von SmartCards ist zusätzlich eine Installation von Treibern und Software clientseitig notwendig. Dadurch sind systembedingte Abhängigkeiten zu berücksichtigen und Aufwand zur Installation mitzuberechnen. Die Übertragung von Login und Passwort wird vom System unterstützt und kann transparent für den Anwender ausgeführt werden, vorteilhaft ist der Ausschluss von Fehlern durch den User selbst z. B. beim Tippen oder durch zeitabhängige Ereignisse.

Zusätzliche Bedingungen:

- SmartCards und Lesegeräte statt Token
- Chipkarte mit Krypto-CoProcessor, RAM, ROM, EPROM
- Gleichzeitige Speicherung von mehreren Schlüsseln, Zertifikaten und statischen Passwörtern
- Kombinierbar als multifunktionaler Firmenausweis
- SmartCard – privater Schlüssel verlässt die Karte nicht
- SmartCard durch PIN geschützt Wissenskomponente
- SmartCard-Lösung verwendet Lesegeräte mit serieller / USB-Anbindung, USB-SmartCards, oder PCMCIA-Reader.

Die ActivIdentity Lösung: SmartCards und Token

Die ActivIdentity Lösung vereint beide Arbeitsweisen und ist damit flexibel einsetzbar. Zum einen realisiert die Tokenlösung für den K-Fall eine einfache und schnelle Handhabung, da keine zusätzlichen Installationen und Systempflege clientseitig notwendig sind; die Integration des Systems kann durch die Einweisung auf die Tokenbenutzung minimiert werden.

Die Telearbeiter verwenden das System regelmäßig mit firmeneigenen Rechnern. Eine Installation von Software zur Steuerung der Smartcard ist daher problemlos möglich. Die Transparenz für den User und die einfache Handhabung gab hier den Ausschlag für die SmartCard.

Die Verwendung von Token und SmartCards ist bei diesem Kunden keine Insellösung, da sie in vielfältiger Weise in die Systemlandschaft integriert werden kann: Als multifunktionaler Firmenausweis genauso wie die Unterstützung von einfache Anmeldeprozeduren oder zertifikatsbasierten Anwendungen.

Die Umsetzung

Für den Einsatz der starken Authentisierung im K-Fall wurde entschieden sowohl eine Management-Konsole als auch die Admin-Datenbank auf den primären Server zu installieren, was im Falle des kompletten Ausfalls der IT-Infrastruktur am Hauptstandort die volle Administrierbarkeit im Back-Up RZ ermöglicht. 400 Anwender wurden für den K-Fall vorkonfiguriert und 30 Telearbeitsplätze mit SmartCards und ActivClient Software ausgestattet.

Die AAA-Server stellen die Komponente der eindeutigen Anwenderidentifizierung dar. Dabei sind die beiden Server als redundantes Hochverfügbarkeits-System (kurz HA-System) konzipiert und installiert worden. Der primäre Server steht im Back-Up RZ, der Backup Server im primären RZ. Auf dem primären Server ist eine administrative Konsole konfiguriert, auf die mittels Terminalserver-Zugriff Änderungen eingepflegt werden können. Die Änderungen können neue Administratoren, User Manager, Help Desk, Profile für die Autorisierung und das Accounting, bestehende Gates, User und Gruppen, bzw. Authentisierungs-devices betreffen.

Die Anwender sind in drei Gruppen eingeteilt; es gibt die Gruppe der Administratoren, die Telearbeiter und die Anwender im K-Fall. In der K-Backup-Gruppe sind 400 Pseudo-Usernamen erfasst und 400 Token zugeordnet. Die Zuordnung der User zu realen Anwendern wird erst im K-Fall vorgenommen. Die Token werden im Back-Up RZ gesichert aufbewahrt und regelmäßig auf Funktionsfähigkeit überprüft. Dies ist insbesondere für die Stromversorgung der Token notwendig, die über austauschbare Batterien verfügen. Dieses Verfahren ermöglicht eine unbeschränkte Nutzungsdauer. Da der Zugangsweg und die Terminalserver-Infrastruktur kontinuierlich von Telearbeitern genutzt werden, sind für diesen Bereich keine Notfallübungen notwendig.

>>>

BDG – make IT safe.

Die BDG GmbH & Co. KG ist seit 1995 ausschließlich auf Dienstleistungen und Projekte der IT-Sicherheit spezialisiert. Die detaillierten Kenntnisse der Sicherheitsrisiken und entsprechender Lösungen resultieren aus der täglichen praktischen Erfahrung mit der Konzeption und Integration sicherer Anbindungen über öffentliche oder private Netze.

BDG steht in engem Kontakt zu den führenden Herstellern. Unabhängig davon beobachten wir den Markt für IT-Security-Produkte sehr gründlich, gehen Trends nach und analysieren neue Technologien und Produkte. Mit diesem Wissen beraten wir unsere Kunden so, dass sie auch in Zukunft die neuen Kommunikationsmedien und -dienste ohne Gefahren nutzen können.

Großbanken, Versicherungen, öffentliche Institutionen und viele mittelständische Unternehmen setzen auf IT-Sicherheit managed by BDG.

Besuchen Sie unsere Webseite unter www.bdg.de oder eine unserer regelmäßig stattfindenden Veranstaltungen – wir haben auch für Ihre speziellen Anforderungen ein offenes Ohr und suchen für Sie die richtige Lösung. Unser Vertrieb freut sich unter sales@bdg.de auf Ihre Kontaktaufnahme.

BDG-Dienstleistungsspektrum

- IT Grundschutz - BS 7799 - ISO 27001
- Security Audits
- Risikoanalysen
- Webapplication Security
- Premium Security Support
- Managed Security Services
- Cooperative Security Management
- Security Policies
- Security Awareness – open-beware!
- IT-Security Solutions Implementation
- Authorised Training Centre
- ITIL Foundation Zertifizierung
- Externer IT-Sicherheitsbeauftragter

BDG-Produktspektrum

- Firewalls & VPN-Systeme
- SSLbased VPNs
- Intrusion Detection und Prevention Systeme
- Content Security Gateways für Web und Email
- Systeme zur Strengen Authentifizierung und für Single Sign On
- Antiviren-Software
- Web Application Firewalls
- Application Acceleration und Delivery Lösungen
- Load-Balancing Systeme

Sicherheit entsteht wenn alle mitmachen!

Mit beware! hat BDG ein professionelles Security Awareness Training entwickelt, mit dem Sie die gesamte Sicherheits-Infrastruktur Ihres Unternehmens verbessern können, indem Sie das Sicherheitsbewusstsein Ihrer Mitarbeiter steigern. Jeder Mitarbeiter kann sich einfach an seinem Arbeitsplatz in zehn Minuten pro Modul schulen!



beware! besteht aus 5 Modulen:

- Passwörter
- Viren
- E-Mails
- Internet
- Vertrauliche Daten

Nutzen Sie zudem die Chance von open source – profitieren Sie von der Weiterentwicklung anderer und stellen Sie Ihre Erweiterungen zur Verfügung.

Für die, die mehr möchten: In der Customized Version erarbeitet BDG mit Ihnen ein ganz persönliches Security Awareness Training: Anpassungen an das Corporate Design, die unternehmensspezifische Security Policy und vieles mehr sind möglich.

Unter www.bdg.de/open-beware können Sie die kostenlose Version von open beware! herunterladen. Der Städte- und Gemeindebund Nordrhein-Westfalen e.V. hat auf der Basis von open beware! das Behörden-IT-Sicherheitstraining BITS entwickelt und stellt es allen Behörden über www.bits-training.de kostenlos zur Verfügung.