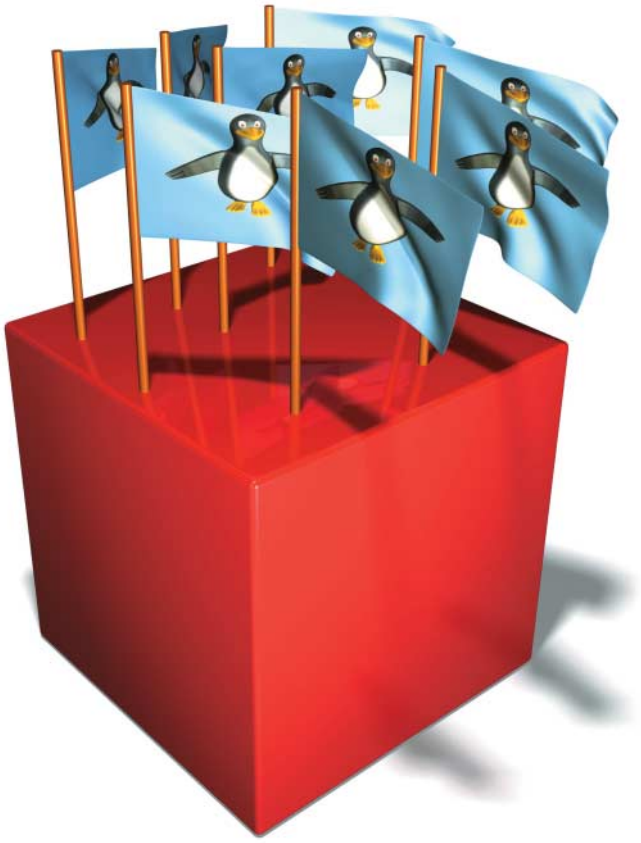


Langzeiterfahrungen
mit 225 000 Linux-Arbeitsplätzen

Eines für alle

Marcus Friedrich

Unbemerkt von der Öffentlichkeit läuft Linux in diversen Geräten wie Routern oder Telefonen. Ähnlich leise verbreitet es sich auf den Desktops. So basieren auf dem Betriebssystem inzwischen circa 225 000 Sparkassen-Arbeitsplätze in ganz Deutschland – zentral versorgt und verwaltet von acht Servern.

Traditionell sind deutsche Sparkassen sehr rechenzentrumslastig orientiert. Das führte zunächst zur Bildung von Buchungsgemeinschaften und regionalen Rechenzentren und schließlich zu einem zentralen IT-Dienstleister, der „Finanz Informatik“ (FI), die ihre Dienste inzwischen für alle deutschen Sparkassen und Partner im Sparkassenverbund erbringt (siehe „Onlinequellen“, [a]).

Bestand der Arbeitsplatz früher noch aus direkt mit dem zentralen Großrechner verbundenen Textterminals mit bernsteinfarbenem Monitor, sind heute grafische Oberflächen gefragt. Auch nahm der Anteil parallel laufender Programme deutlich zu, die sich nicht nur auf die Bankfachlichkeit beschränken, sondern auch Produktivitätswerkzeuge wie Browser, E-Mail sowie Office- und individuelle Anwendungen umfassen. Die Erfahrungen aus einigen Jahren OS/2 zeigten, dass man um Windows als Systemplattform nicht herumkommt, dabei aber durch den Einsatz von Terminalservern die Vorteile der Zentralisierung ausnutzen kann. Das reduziert die dezentralen Infrastrukturen auf ein sinnvolles Maß und erhält trotzdem alle notwendigen Funktionen. Durch die Nutzung des Windows-Aufsatzes „XenDesktop“ von Citrix ist zumindest am Endgeräteansatz eine Unabhängigkeit von Microsoft gegeben. Der Grundstein für eine mögliche, fast unsichtbare Linux-Nutzung am Client ist gelegt, ohne die gewohnte Betriebsweise zu verlassen.

Ziel der Endgeräteplattform der Finanz Informatik war ein möglichst schlanker Client, der ausschließlich den Citrix-Betrieb nutzt, analog einer Blackbox, gemäß „aufstellen, einschalten, nutzen“. Dieser Ansatz mag zwar theoretisch verlockend klingen, ist aber im großen Stil nicht durchzuhalten. Individuelle Einstellungen wie Links-/Rechtshändermaus mögen noch verkraftbar sein, bei Sicherheitsupdates mag man aber nicht alle Blackboxes austauschen gehen. Gerade die jüngst bekannt gewordenen Sicherheitslücken im SSL- oder Shellshock-Umfeld zeigen, wie schnell man bei allen Geräten unabhängig vom Betriebssystem handeln muss.

Solche schlanken Clients bezeichnet man zwar oft als Thin Client, wobei das „thin“ heutzutage meist nur die kleine Hardware betrifft. Softwareseitig ist inzwischen deutlich mehr als nur Betriebssystem und Citrix-Client enthalten. Dazu später mehr.

Zentrales Management ist Pflicht

Die Gretchenfrage bei größeren Installationen ist immer „Kostenersparnis durch Standards versus Kosten der Individualität für den Benutzer“. Natürlich beantwortet das jeder Administrator mit „Standard“, sprich: jeder Arbeitsplatz ist identisch. Der Benutzer will aber eigene Hintergründe, Bildschirmauflösungen, Bildschirm-

iX-TRACT

- Rund 225 000 Linux-Clients lassen sich mit acht Servern verwalten.
- Bei diesen Stückzahlen muss ein zentralisiertes Managementsystem mit den Lastspitzen skalieren können.
- Auch bei Linux-Clients darf man das Security-Management nicht unterschätzen.
- Die stetig wachsende Stückzahl bestätigt die Linux-Strategie der Finanz Informatik.

schoner, individuelle Anwendungen et cetera. Einen Ausweg liefert nur ein Verwaltungssystem, das per Endpunkt am Client diesen konfiguriert und versorgt. Dieses Kernstück einer solchen Umgebung muss gut durchdacht sein, ist doch ein nachträglicher Wechsel der Infrastruktur mit extremem Aufwand verbunden.

In der Finanz Informatik entschied man sich im Jahre 2006 für das System der Karlsruher Firma Unicon [b]. Zusätzlich zu ihrer zentralen Managementsoftware „Scout Enterprise“ hat die Firma mit „eLux“ ein Endgerätebetriebssystem mit passendem Management-Endpunkt im Portfolio. eLux basiert auf Linux und läuft gemäß Hersteller auf diversen Hardwaretypen unterschiedlicher Lieferanten. Gerade die Hardwareunabhängigkeit ist zum einen wichtig, um den Vorlieben der einzelnen Kunden nachzukommen, aber zum anderen auch um Unabhängigkeit von Lieferengpässen oder Geräteserienproblemen zu erhalten. Nicht zuletzt gibt der durch Rahmenverträge mit den Herstellern garantierte Preis Investitionssicherheit.

Derzeit sind 29 Modelle der Hersteller Lenovo, Fujitsu, HP, IGEL, VXL und Samsung von der Finanz Informatik durch einen Validierungsprozess freigegeben, wobei die Hersteller meist zwei Jahre Lieferbarkeit und weitere fünf Jahre Support garantieren. Für diese rund sieben Jahre erhält auch das Client-Betriebssystem Pflege und Wartung.

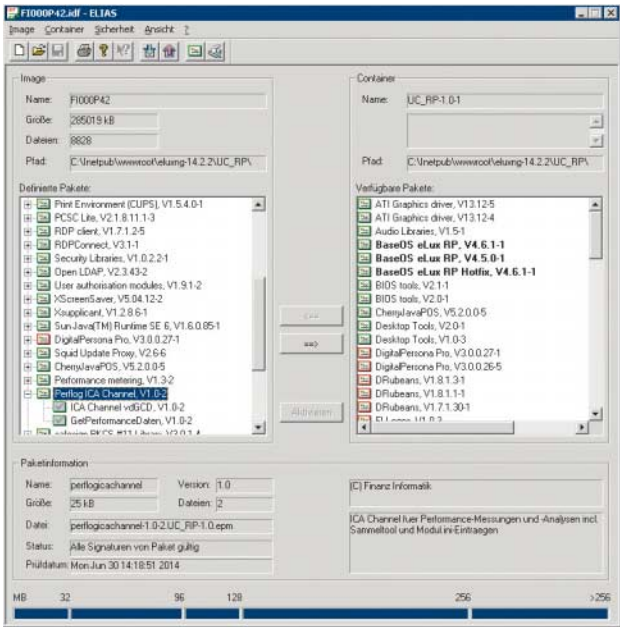
Endgeräteversorgung und Konfiguration

Ähnlich den üblichen Linux-Distributionen wie Debian mit *.deb oder Red Hat mit *.rpm existiert auch für eLux ein Paketformat: *.epm/*.fpm. Darüber lassen sich ebenfalls nicht nur Komponenten oder Funktionen einspielen respektive deinstallieren, sondern es versucht auch, Abhängigkeiten aufzulösen. Die Summe der notwendigen Komponenten fließt in eine Image-Definition zusammen, die letztendlich die eigentliche Betriebssystem-Firmware der Clients repräsentiert.

Deren Komposition erfolgt über ein weiteres Tool: ELIAS (siehe Abb. 1). Will man nur ein einzelnes Programm auf den Clients erneuern, so ist auch nur dieses in der Image-Definition zu aktualisieren. Ein Software-Update zieht dann ausschließlich die Nachversorgung dieses Programms nach sich. Gerade bei mit geringer Bandbreite angebundenen Zweigstellen reduziert dies den Netzwerkverkehr erheblich.

Zum zentralen Verwalten dieser Clients dient das schon erwähnte Managementsystem Scout. Dieses Server-Tool läuft auf acht zentralen Windows 2012 Servern an zwei Standorten in Deutschland und benutzt eine SQL-Datenbank, die sämtliche Verwaltungsinformationen speichert. Per Scout lässt sich nicht nur das Linux-Betriebssystemmanagement (Software-Sollzustand und Betriebssystemkonfiguration) erledigen, sondern es erlaubt auch das Verwalten aller für den Client sichtbaren Anwendungen inklusive deren Konfigurationen und Lizenzen. Ein Sortieren in übersichtliche logische Gruppen verhindert, dass man die Übersicht über die Geräte verliert. Diese Organisationseinheiten (OU) genannten Gruppen lassen sich ähnlich wie in Microsofts Active Directory in einer Baumstruktur anlegen. Da alle Geräte ihre Eigenschaften wie Hardwaretyp, BIOS-Version, angeschlossene Monitore oder USB-Geräte, Auflösung et cetera bei jedem Bootvorgang an den Scout-Server melden, lässt sich auch ein Reporting auf die einzelnen OUs fahren.

Über Online-Kommandos kann man sowohl an einzelne Geräte als auch an ganze OU-Bäume diverse Befehle senden, wie Einschalten per Wake On LAN, Ausschalten beziehungsweise Reboot, Software-Update, Nachricht, Konfiguration neu versorgen, Benutzeroberfläche spiegeln et cetera. Ein für die FI weiteres wichtiges Kommando ist „Diagnosedateien anfordern“. Hiermit lassen sich von einer zentralen Stelle aus individuelle technische Dateien aus dem Dateisystem der Endgeräte abziehen sowie parallel Unix-Befehle auf den Clients ausführen und deren Ausgabe einsammeln. Dies ist für die Fehlersuche extrem nützlich, da man beispielsweise schnell funktionierende mit nicht funktionierenden Geräten vergleichen oder über die gezielte Log-Dateianalyse das Problem offline und somit ohne Benutzerinteraktion identifizieren kann.

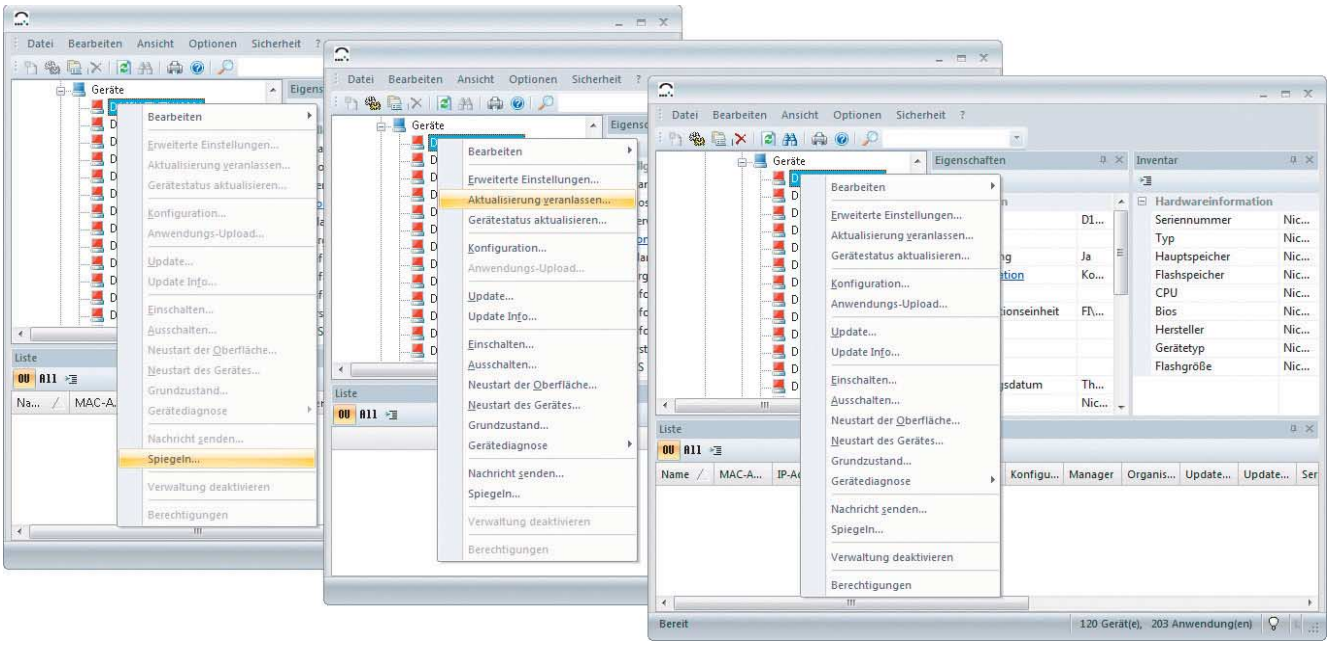


Modulare Firmware-Zusammensetzung per Tool ELIAS (Abb. 1)

Versierte Administratoren wissen sicherlich, dass man manche Problemmeldungen per Mail oder per Telefon nicht richtig interpretiert, was eine Visualisierung notwendig macht. Diese sowohl vom Rechenzentrum als auch vom lokalen Administrator des Kunden initiierte Spiegelung der teilweise weit entfernten Endgeräteoberfläche benötigt jedoch die Mithilfe des davorsitzenden Benutzers. Dieser erteilt die Erlaubnis und kann jederzeit die Sitzung abbrechen. Üblicherweise ist der Spiegelnde parallel per Telefon mit dem Benutzer verbunden, sodass der Benutzer die reproduzierbaren Fehlerschritte vorführen und der Spiegelnde gegebenenfalls Analyseaktionen erklären kann. Dies ermöglicht komfortabel die Analyse sowohl der Windows-Server- als auch der Linux-Probleme. In ganz seltenen Fällen kann es notwendig sein, ein Endgerät physisch an die Entwicklung der Finanz Informatik zu senden, um es hardwareseitig oder forensisch zu analysieren respektive mit den Referenzsystemen zu vergleichen.

Mandantenfähigkeit und Rollenverwaltung

Aufgrund unterschiedlicher Aufgabenrollen besteht der Bedarf für den Zugriff auf die Scout-Funktionen nicht nur bei den Mitarbeitern im Rechenzentrum, sondern auch bei den dezentralen Institutsadministratoren und Supportmitarbeitern. Dazu müssen diese eine entsprechend aktuelle Version der Scout-Konsole auf einen Windows-Administrations-Client oder in die Terminalserver-Farm installieren und einer ihren Tätigkeiten zugehörigen AD-Benutzergruppe zuordnen. Dabei benutzt die Finanz Informatik in den Scout-Berechtigungen je zwei Instituts- und Re-



Rechtestruktur in Bezug auf Scout (v. l. n. r.): Helpdesk-User, Institutsadministrator, Rechenzentrumsadministrator (Abb. 2)

chenzentrumsgruppen sowie eine Root-Gruppe. Letztere verfügt natürlich über volle Rechte an Scout, während die Rechenzentrumsgruppen alle Kunden und die Kundengruppen nur ihr Institut sehen und verwalten können. Der einen Rechenzentrumsgruppe bleibt ausschließlich das Recht zum Spiegeln der Endgeräte, was üblicherweise die Helpdesk-Supporter nutzen. Die zweite Gruppe ist für übliche Administrationsaufgaben gedacht. Die sensitiven Aufgaben bleiben der Root-Gruppe vorbehalten.

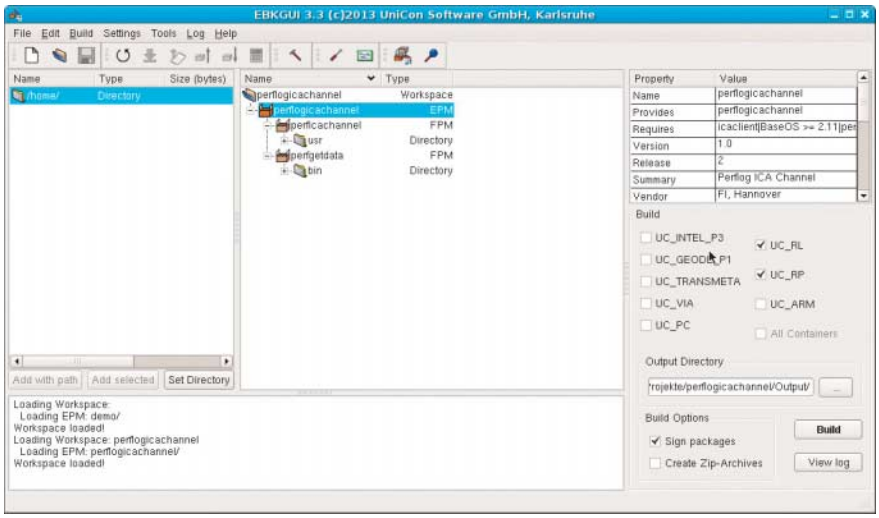
Je nach Gruppenmitgliedschaft modelliert sich die Menüstruktur beziehungsweise das Kontextmenü in der Scout-Konsole (siehe Abb. 2). Da die Berechtigungen mit internen Scout-Mitteln realisiert sind, muss die Finanz Informatik bei jedem Einsatz einer neuen Scout-Version, die neue Menüs mitbringt, auch die Berechtigungen in Scout anpassen. Allerdings ist die Datenbankstruktur recht gut dokumentiert, sodass nach der Installation der neuen Bits ein SQL-Skript ausreicht, die Rechte über alle Institute neu zu setzen.

Clientseitige Hardware- und Softwareerweiterungen

Ein weiterer Aspekt ist der Anschluss diverser bankenspezifischer sowie standardisierter Peripheriegeräte an den Endgeräten der Kunden. Die Palette reicht von großen und extrem schweren Kassentresoren über serielle Sparbuchdrucker und Unterschriften-Pads bis hin zu Biometrie- und Smartcard-Lesern. Während die älteren Geräte meist über serielle Anschlüsse verfügen, nutzen die neueren USB. Das bedingt allerdings auch, dass die Gerätetreiber auf dem Linux-System installiert sein müssen. Üblicherweise ist eine zusätzliche Gerätesteuerungskomponente notwendig. So erfolgt die Kassensteuerung beispielsweise per Java-Device-Steuerung, während das Smartcard-Paket den Open-Source-Daemon *pcsc* und die Biometrie-Anwendung proprietäre Komponenten zweier Hersteller nutzt.

Neben diesen hardwarenahen Komponenten sind auch einige Softwarepakete notwendig. Zu den klassischen Terminalserver-Bausteinen wie Citrix- und RDP-Client gesellen sich Mobilitätskomponenten wie ein VPN-Client oder AnyConnect von Cisco. Je nachdem, welche Verträge die Finanz Informatik mit den jeweiligen Herstellern hat, liefern diese die zugehörigen Pakete entweder selbst oder lassen sie durch Unicon paketieren.

In einigen Fällen programmiert jedoch auch die Finanz Informatik eigene Erweiterungen für das Linux-Betriebssystem, angefangen bei einigen Bash-Skripten über Citrix Virtual Channels bis hin zu C++-Tools für zentralisierte Performance-Messungen. Mit dem Paketierungsstudio „eLux Builder Kit“ von Unicon lassen sich diese Erweiterungen im *epm-/*fpm-Format paketieren (siehe Abb. 3). Hier zeigt sich im Vergleich zwischen Windows- und Linux-Clients kein Unterschied. Ändert Citrix seine APIs oder wird ein neues Betriebssystem und somit ein neuer Linux-Kernel fällig, müssen die



eLux Builder Kit zum Selbstbau von Paketen (Abb. 3)

Administratoren das Entwicklungssystem aktualisieren und den Compiler sowie das Paketierungstool erneut anwerfen.

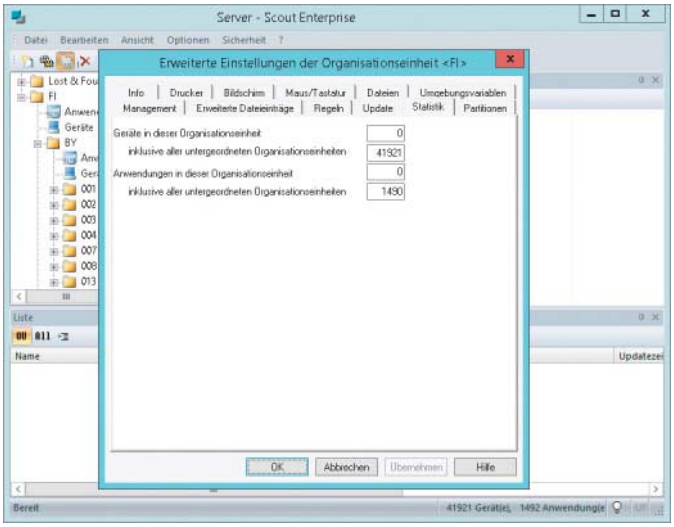
Security-, Patch-, Alert-Management

Gerade im Hinblick auf Security genießt Linux einen guten Ruf. Nach fast zehn Jahren produktiver Erfahrungen zeigt sich jedoch, dass man dieses Thema auch bei Linux nicht unterschätzen darf. Die Finanz Informatik ist Mitglied im Alert-Service S-CERT der SIZ GmbH, einer von Institutionen der Sparkassen-Finanzgruppe gemeinsam betriebenen Firma [c]. Dort beobachtet und bewertet man unter anderem Sicherheitsmeldungen sowohl von Betriebssystemen (Windows und Linux) als auch von Anwendungen und informiert die angeschlossenen Institute.

Während sich die Alerts bei Windows zu 95 % auf den monatlichen Patchday konzentrieren und man dort üblicherweise alle Patches möglichst schnell installiert, listet das SIZ bei Linux inklusive der Open-Source-Programme ungefähr fünf bis zehn Meldungen pro Tag auf. So oft wird niemand patchen wollen und oft auch nicht können, sodass die Finanz Informatik diese Alerts genauestens analysieren muss. Meist gibt es Abhängigkeiten zu den Programm- oder Kernel-Versionen, die eine Entscheidung über die Notwendigkeit vereinfachen. Manchmal muss man allerdings tief in den Open-Source-Quelltext schauen, um zu verstehen, ob sich die Bedrohung ausnutzen lässt oder ob andere Sicherheitsmaßnahmen greifen.

Kommt der Alert von einem Hersteller, der die Sicherheitsprobleme nicht offenlegt, etwa Java von Oracle, AnyConnect von Cisco oder der Receiver von Citrix, ist das Linux-System umgehend zu aktualisieren. Gerade bei 225 000 Endgeräten bedeutet das immer eine große Herausforderung, die auch eine Erfolgskontrolle einschließen muss. Erfahrungsgemäß kommen im Jahr zu den geplanten halbjährlichen Release-Terminen für neue Software im Schnitt weitere vier Update-Termine durch Security-Alerts.

Aus diesem Grund ist es wichtig, dass nur die Geräte in das Verbundnetz gelangen, die dem Institut und der Finanz Informatik bekannt sind. Neben den physischen und baulichen Zugangsschutz zum Netz gesellt sich eine „Zwangs“-Vorabgenerierung der Linux-Clients. Die stellt sicher, dass unbekannte eLux-Geräte in einer Scout-OU landen, die das Gerät so lange deaktiviert, bis die Generierung erfolgt ist. Zusätzlich überprüft der Client bei der Erstinbetriebnahme seine Software und aktualisiert sie gegebenenfalls automatisch.



40 000 Clients werden mit einem Managementserver verwaltet (Abb. 4).

Kritische Update- und Betriebsverfahren

Neben den Security-Updates kommt man bei der oben erwähnten Hardwarelaufzeit von bis zu sieben Jahren um einen Betriebssystemwechsel nicht herum. Gerade neuere Hardwaretypen bedingen immer aktuellere Treiber, die nicht mehr auf den alten Kernel-Versionen laufen. Dadurch ist die Finanz Informatik derzeit gezwungen, drei eLux-Versionen im Einsatz zu haben. Zum Reduzieren des Aufwands für Wartung und Pflege der Versionen stehen auch bei alter Hardware Zwangsmigrationen auf den neuen Kernel an, was eine komplette Neuinstallation der Geräte bedeutet. Dabei stellt der Hersteller ein Update-Verfahren zur Verfügung, das mit einer minimalen Linux-Wartungsinstanz das System automatisch aktualisiert. Dieses berücksichtigt die von der Finanz Informatik per Whitelist freigegebenen Hardwarekomponenten. Leider erreicht man bei solchen kritischen Updates nicht die gleiche Erfolgsrate wie bei normalen Updates, da aufgrund der Stückzahlen die Infrastruktur stark belastet wird. Für die wenigen ausgefallenen Geräte, die per Netzwerk nicht mehr erreichbar sind, bleibt dann nur eine Neuinstallation per USB-Stick.

Onlinequellen

[a] Finanz Informatik GmbH & Co. KG
www.f-i.de

[b] Unicon Software GmbH
www.unicon-software.com

[c] S-CERT des SIZ
siz.de/sicherheit/produkte-uebersicht/s-cert.html

Die Finanz Informatik hat die Belastung der Infrastruktur schon früh erkannt und migriert serverseitig gerade von einer 32-Bit-Basis auf ein 64-Bit-Windows mit 64-Bit-SQL-Serverinstanz. Mit weiteren internen Scout-Optimierungen zeigt sich nach den ersten zwei Serverumstellungen ein Rückgang der lastbasierten Ausfälle um 95 %, sodass einem weiteren Client-Zuwachs nichts mehr im Wege steht.

Fazit und Ausblick

Die Linux-Clients haben den Windows-Clients bislang nur ein Feld wieder überlassen. Im zum Vergleich zum Desktop deutlich schnelllebigeren Notebook-Bereich zeigte sich, dass die Linux-Treiber nicht so hochwertig und zeitnah wie bei Windows zur Verfügung standen, sodass, bedingt durch den internen Qualitätssicherungs- und Freigabeprozess, die Hardware nur noch wenige Monate lang lieferbar war. Auch ist eine Offlinefähigkeit mit lokal installierten E-Mail- und Office-Produkten nur mit Windows-Clients gegeben.

Neben der derzeitigen Herausforderung der flächendeckenden Migration aller Endgeräte auf die neue einheitliche Kernel-Version stehen weitere für den Linux-Client vor der Tür: IP-Telefonie und Multimedia werden die Hauptthemen für 2015 sein, die auch sicherheitstechnisch einiges an Arbeit mitbringen werden. (avr)

Dipl. Ing. Marcus Friedrich

arbeitet bei der Finanz Informatik und ist Leiter des Clientteams, das sowohl die Basisplattform der Windows-Clients als auch die Systemplattform der Linux-Clients inklusive Managementserver für die deutschen Sparkassen bereitstellt.

Alle Links: www.ix.de/ix1503080