

Risiken Individueller Datenverarbeitung (IDV) in Banken von Roy von Rango

Die Entwicklung von Anwendungen erfolgt nicht nur in der zentralen IT, sondern zunehmend auch in Fachbereichen der Banken. Entwicklung, Betrieb und Dokumentation dieser Anwendungen entsprechen dabei häufig nicht den Vorgaben der zentralen IT an von ihr selber entwickelte und/oder betriebene Anwendungen. Erfüllt die zentrale IT in der Regel die meisten gesetzlichen und/oder regulatorischen Anforderungen, ist dies bei Anwendungen, die vom programmierenden Endanwender erstellt werden, überwiegend nicht der Fall. Dieser Artikel beschäftigt sich mit grundlegenden Fragen zum Einsatz von IDV (Individueller Datenverarbeitung) in Bereichen, die besonderen gesetzlichen und/oder regulatorischen Anforderungen unterliegen. Dieses geschieht am Beispiel eigenerstellter Excel-Anwendungen, d. h. sowohl einfacher Excel-Sheets als auch mit Hilfe von VBA programmierten komplexen Excel-Anwendungen, unter Bezug auf die Empfehlungen des BSI, als einem der in der MaRisk geforderten gängigen Standards, sowie der IDW RS FAIT 1.

IDV ist dadurch gekennzeichnet, dass der Endanwender in einem Unternehmen mit Hilfe der ihm zur Verfügung stehenden Werkzeuge eigenständig technische Lösungen für seinen Aufgabenbereich erstellt, die seinen fachlichen Anforderungen entsprechen (programmierender Endanwender). Dies geschieht meist ohne Beachtung der in der IT üblichen Prozesse hinsichtlich Entwicklung, Betrieb und Dokumentation von Anwendungen. Excel-Anwendungen stellen klassische IDV dar.

Die **MaRisk**, eine im Bankenbereich zentrale Vorgabe, fordert, dass die IT-Systeme (Hardware und Software) und die zugehörigen IT-Prozesse die Integrität, Verfügbarkeit, Authentizität sowie die Vertraulichkeit der Daten sicherstellen müssen. Für diese Zwecke ist bei der Ausgestaltung der IT-Systeme und der zugehörigen Prozesse grundsätzlich auf gängige Standards abzustellen (AT 7.2, 2.).

Das **BSI**, einer der beiden vom BaFin explizit genannten Standards, thematisiert in der Maßnahme M 2.379 des IT-Grundschutzkatalogs die Softwareentwicklung durch den Endanwender unter explizitem Bezug auf die Programmierung unter Microsoft.

Die Empfehlungen des BSI zielen darauf ab, zunächst zu entscheiden, ob überhaupt Eigenentwicklungen durch den Endanwender in der Bank zugelassen bzw. erwünscht sind. Wenn ja, ist zu klären, unter welchen Voraussetzungen diese erfolgen und in welche Entwicklungs-, Betriebs- und Kontroll-Prozesse sie eingebunden werden sollen. An dieser Stelle des Grundschutzkatalogs gibt das BSI keinen expliziten Hinweis darauf, dass IDV ungeeignet für die Umsetzung bestimmter gesetzlicher und/oder regulatorischer Anforderungen sei. Die Empfehlung lautet, dass, wenn Eigenentwicklungen durch den Endanwender erlaubt sind, entsprechende Richtlinien entwickelt werden sollten, um Mindestanforderungen an Sicherheit, Dokumentation und Qualität sicherzustellen. Dies könnte implizit so interpretiert werden, dass das BSI IDV nicht für alle gesetzlichen und/oder regulatorischen Anforderungen als geeignet ansieht.

Entsprechend steht an einer anderen Stelle des Grundschutzkatalogs (M 2.223), dass Office-Produkte nicht für jeden beliebigen Einsatzzweck geeignet sind. Gemeint ist hier generell Büro-Standardsoftware, mit der typische Büroaufgaben erledigt werden, also auch Microsoft-Excel. An dieser Stelle geht das BSI jedoch nicht explizit auf die Programmierung unter Excel ein.

Insofern lässt das BSI zumindest Zweifel am Einsatz von IDV in Bereichen mit besonderen gesetzlichen und/oder regulatorischen Anforderungen. Diese Zweifel sind nicht unbegründet, denn völlig unabhängig davon, welche Excel-eigenen Schutzmaßnahmen (Arbeitsmappenschutz, Blattschutz etc.) implementiert sind, kann Excel die Integrität, die Authentizität sowie die

Vertraulichkeit der Daten mit „Bordmitteln“ nicht sicherstellen. Der mit Excel-eigenen Mitteln zu implementierende Schutz schützt die Daten lediglich vor ungewollter Veränderung. Excel kann keine Informationen vor vorsätzlichen Angriffen schützen, obwohl es diese Illusion vermittelt. Der Schutz der Daten in Excel entspricht dem einer verlorenen oder gestohlenen EC-Karte, auf die der Eigentümer den PIN notiert hat. So kann z. B. der Blattschutz mit Excel-eigenen Mitteln durch jeden Mitarbeiter, der Zugriff auf das Sheet hat, durch einfaches „Copy & Paste“ überwunden werden – quasi legal, mit wenigen Schritten. Ganz abgesehen davon, dass es Dutzende von im Internet frei verfügbaren Programmen gibt, die illegal jeden mit Excel-Bordmitteln erstellten Schutz überwinden, indem sie Passworte „knacken“ oder diese gleich ganz entfernen.

Wenn also Eigenentwicklungen durch den Endanwender zugelassen werden, sollte dem programmierenden Endanwender, der i. d. R. kein geschulter Programmierer ist, Unterstützung zuteilwerden. Der Endanwender muss u. a. in die Lage versetzt werden, die Kritikalität eines in seinen Augen möglicherweise einfachen und nur der Arbeitserleichterung dienenden Excel-Sheets zu beurteilen, um die Einhaltung der jeweiligen gesetzlichen und/oder regulatorischen Vorgaben zu gewährleisten.

In der Praxis zeigt sich, dass die Kritikalität von eigenerstellten Excel-Anwendungen unter Verweis darauf, es handele sich nur um eine Arbeitserleichterung, die man jederzeit durch „manuelles Rechnen“ ersetzen könne, vielfach unterschätzt wird. In Excel-Anwendungen ist häufig über Jahre erworbenes hohes fachliches und technisches Know-how verarbeitet. Aufgrund der oft lückenhaften oder gänzlich fehlenden fachlichen und technischen Dokumentation ist ein adäquates manuelles Rechnen, das möglicherweise sogar kurzfristig erforderlich wird, gar nicht mehr unmittelbar möglich. Dieses gilt vor allem dann, wenn der programmierende Endanwender, der sehr häufig fachliches und technisches Know-how in einer Person vereint, plötzlich ausfällt.

Zweckmäßigerweise sollte daher eine IDV-Richtlinie erstellt werden, die die Kritikalität der in der Bank verwendeten IDV in Bezug auf relevante gesetzliche und/oder regulatorische Vorgaben klassifiziert und, davon abhängig, Vorgaben für die Entwicklung, den Betrieb und die Dokumentation der IDV definiert. Notwendige Voraussetzung ist die Erfassung sämtlicher IDV in einer Anwendungsliste. Es sollten hier die Verfahren greifen, die im Bereich der operativen Datenverarbeitung (ODV) allgemein üblich sind.

Eine darüber hinausgehende und für den ungeschulten Programmierer wesentliche Unterstützung ist, ihm anhand von qualitätsgesicherten Code-Beispielen – zentral abgelegt in entsprechenden Bibliotheken – Lösungsmöglichkeiten zu geben, mit denen spezielle, durch die gesetzlichen und/oder regulatorischen Regelungen vorgegebene Anforderungen umgesetzt werden können. Als Beispiel sei hier genannt, wie man in Excel mit Hilfe von VBA Änderungen protokollieren oder einen tatsächlichen Zugriffsschutz implementieren kann.

Entsprechenden Code kann der programmierende Endanwender auch aus dem Internet beziehen. Dieser ist jedoch häufig nur schwer zu verstehen und vor allem nicht qualitätsgesichert. Es ist absolut vorstellbar, dass bei Nutzung von Quellcode aus dem Internet schadhafter oder boshafter Code in die Anwendung gerät – vom programmierenden Endanwender unbemerkt.

In diesem Zusammenhang fordert die MaRisk ebenfalls, dass IT-Systeme vor ihrem erstmaligen Einsatz und nach wesentlichen Veränderungen zu testen und von den fachlich sowie den technisch zuständigen Mitarbeitern abzunehmen sind. Hierfür ist ein Regelprozess der Entwicklung, des Testens, der Freigabe und der Implementierung in die Produktionsprozesse zu etablieren. Produktions- und Testumgebungen sind dabei grundsätzlich voneinander zu trennen (AT 7.2, 3.).

Entsprechende Empfehlungen gibt auch das BSI in seinem Maßnahmenkatalog M 2.378. Demnach

müssen auch Eigenentwicklungen getestet und freigegeben werden, bevor sie in der Produktivumgebung eingesetzt werden dürfen. Ebenso muss geklärt werden, wer die Programme wartet und Probleme damit behebt. Insofern erfordert eine Unterstützung des programmierenden Endanwenders auch ein professionelles Test-Management sowie eine begleitende Qualitätskontrolle durch einen geschulten Programmierer oder eine andere Instanz (z. B. ein Kollektiv aller programmierenden Endanwender des Unternehmens). Die Durchführung von Entwicklertests, so wie es bei IDV – wenn überhaupt – üblich ist, ist für Anforderungen des BSI nicht ausreichend. Dieses gilt umso mehr, als IDV i. d. R. auch in der Produktivumgebung entwickelt und getestet wird. Daher sollte zumindest die Trennung zwischen Entwicklungs-, Test- und Produktionsumgebung durch unterschiedliche „produktive“ Laufwerke sowie ein geregeltes Transportverfahren zwischen diesen Laufwerken und unterschiedliche Zugriffsrechte auf die Laufwerke gewährleistet sein.

In den Hilfsmitteln des Grundschutzkatalogs ist eine Richtlinie der Bundesknappschaft zur „PC-Anwendungsentwicklung durch den Endbenutzer“ veröffentlicht, die laut BSI „den Einsatz von selbstentwickelten Anwendungsprogrammen (z. B. Makros) durch PC-Benutzer regelt, damit auch im Rahmen einer individuellen Datenverarbeitung der Einhaltung bestehender Vorschriften zum Datenschutz und zur Datensicherheit Rechnung getragen wird.“ Somit bestätigt das BSI letztendlich die Möglichkeit, Excel-Anwendungen konform mit den Vorgaben besonderer gesetzlicher und/oder regulatorischer Vorgaben zu gestalten – trotz der angesprochenen Zweifel, die aus dem Maßnahmenkatalog des Grundschutzkatalogs deutlich werden. Hinweise zum Testmanagement fehlen hier.

Allerdings ist auf jeden Fall VBA-Programmierung oder der Einsatz entsprechender zusätzlicher Tools, die aber im Grunde nichts anderes als VBA-Code sind, erforderlich. Für die Anwendungsentwicklung benötigen die programmierenden Endanwender – wie oben ausgeführt – Unterstützung in Form einer entsprechenden Organisation sowie von Regelwerken, mit deren Hilfe die Sicherheit, die Qualität und die Konformität mit den jeweiligen gesetzlichen und/oder regulatorischen Anforderungen gewährleistet werden kann.

Es entspricht durchaus der Best Practice, dass bei Verwendung von IDV die bei der zentralen IT üblichen Prozesse hinsichtlich der Entwicklung, des Betriebs und der Dokumentation vom Fachbereich übernommen bzw. adaptiert werden und dass möglicherweise der Betrieb, abhängig von der Kritikalität der Anwendung, an IT übergeht. Dies ist auch in der Richtlinie der Bundesknappschaft so vorgesehen.

Ein im Vergleich zum BSI spezialisierterer Standard, die „Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie“ (**IDW RS FAIT 1**) definiert den Begriff „Informationstechnologie“ als die Gesamtheit der im Unternehmen zur elektronischen Datenverarbeitung eingesetzten Hard- und Software. Eine explizite Unterscheidung zwischen IDV und ODV findet nicht statt, wodurch die zentrale Rolle der IT betont wird, ohne die Möglichkeit der Einbindung programmierender Endanwender in den Fachbereichen auszuschließen. Allerdings wird darauf hingewiesen, dass eine funktionale Trennung sowohl innerhalb des IT-Bereichs (Entwicklung und Betrieb) als auch zu anderen Abteilungen des Unternehmens bestehen sollte. „Sollte eine solche Funktionstrennung nicht möglich sein, z. B. bei Personalidentität zwischen Fach- und IT-Aufgaben“, was bei programmierenden Endanwendern der Fall ist, „sind zusätzliche Überwachungsmaßnahmen einzurichten“. Diese zusätzlichen Überwachungsmaßnahmen sollten in der zu erstellenden IDV-Richtlinie dokumentiert werden.

Die Verwendung von VBA-Code aus dem Internet muss auch in Hinsicht auf lizenzrechtliche Kriterien betrachtet werden. Wird VBA-Code aus dem Internet gezogen und in der Bank verwendet, handelt es sich um FOSS. Lizenzverstöße bei lizenzrechtlich ungeprüfter Verwendung von VBA-

Code aus dem Internet sind nicht völlig auszuschließen. Insofern sollte die Verwendung von FOSS – explizit auch die Verwendung von VBA-Code aus dem Internet – in dem Lizenzmanagement der Bank geregelt sein. Hier können auch die entsprechenden Prozesse zur Prüfung der Sicherheit und der Qualität der jeweiligen Anwendungen oder Code-Passagen sowie deren lizenzrechtliche Unbedenklichkeit verankert sein.

Fazit:

Auch mit eigenerstellten Excel-Anwendungen lassen sich die Vorgaben des BSI sowie der IDW RS FAIT 1 umsetzen. Dieses ist allerdings nicht mit Excel-eigenen Mitteln zu erreichen, sondern erfordert den Einsatz von VBA (oder entsprechender Zusatztools).

Es sollten Regelwerke und, daraus abgeleitet, organisatorische Regelungen zur Erstellung von Excel-Anwendungen entworfen werden, u. a. um Sicherheitsmängeln durch aus dem Internet importierten VBA-Schadcode (bzw. nicht ausreichend qualitätsgesicherten und getesteten eigenen Code) sowie möglichen Lizenzverstößen vorzubeugen und die Konformität mit den Vorgaben der Standards zu gewährleisten.

Dazu ist die Übernahme oder Adaption der bei der zentralen IT üblichen Prozesse hinsichtlich Entwicklung, Betrieb und Dokumentation (einschließlich der üblichen Testverfahren) durch den Fachbereich und ggf. die Übergabe des Betriebs an die zentrale IT erforderlich. Dieses beinhaltet auch die bei IDV ebenfalls mögliche Trennung zwischen Entwicklungs-, Test- und Produktionsumgebung sowie die Sicherstellung der lizenzrechtlichen Unbedenklichkeit bei Verwendung von VBA-Code aus dem Internet durch Aufnahme in das Lizenzmanagement der Bank.

Die Vorteile für die Bank aus einer entsprechenden Organisation sind:

- ***Know-how-Übertragung zwischen den einzelnen häufig isoliert voneinander arbeitenden programmierenden Endanwendern in den einzelnen Fachbereichen***
- ***dadurch bessere Gewährleistung von Stellvertreter-Regelungen***
- ***sicherer und qualitativ höherwertiger Code***
- ***bank-einheitlicher Code***
- ***geringerer Programmier- und Pflegeaufwand***
- ***höhere lizenzrechtliche Sicherheit und letztendlich***
- ***bessere Gewährleistung der Einhaltung gesetzlicher und/oder regulatorischer Vorgaben.***

Sinnvoll ist die Erstellung einer Code-Bibliothek mit qualitätsgesicherten Code-Passagen oder ganzen Programmen zur Umsetzung der Einhaltung der Vorgaben beider Standards (z. B. Änderungsprotokollierung, Gewährleistung des Zugriffsschutzes).

Roy von Rango ist als freiberuflicher IT-Auditor u. a. für CDC Compliance & Datenschutz Consulting UG (haftungsbeschränkt) tätig.