KNUT HÜNECKE · ROLAND SCHÄFER

Computer-Führerschein und Datenschutz

Der ›Europäische Computer-Führerschein‹ hat sich als standardisiertes Verfahren der informationstechnischen Qualifikation durchaus Anerkennung erworben – im Hinblick auf Datenschutz aber gibt es die Note ›mangelhaft‹!

Der ›Europäische Computer-Führerschein‹ soll ein Nachweis sein für umfassende Kenntnisse im Umgang mit dem Computer. International läuft das Zertifikat unter dem Begriff ›European Computer Driving Licence‹, kurz ECDL, und basiert auf einer Initiative des ›Council of European Professional Informatics Societies‹ (CEPIS) in Zusammenarbeit mit der Europäischen Union (EU), wobei Bundesbildungsministerin Edelgard Bulmahn hierzulande die Schirmherrschaft über den ECDL übernommen hat. In Deutschland bereiten inzwischen rund 800 Trainingszentren auf den Erwerb des ECDL vor. Sie sind auch berechtigt, die entsprechenden Prüfungen abzunehmen.

Praxisbezogenes Wissen soll im Vordergrund stehen bei den sieben Teilprüfungen, aus denen sich der ECDL zusammensetzt. Im Einzelnen untergliedern sich diese Einheiten in folgende Lernfelder:

- Grundlagen der Informationstechnologie,
- Computernutzung und Dateiverwaltung,
- Textverarbeitung,
- Tabellenkalkulation,
- Datenbanken,
- Präsentation,
- Informations- und Kommunikationsnetze.

Jede erfolgreich abgeschlossene Teilprüfung wird in die so genannte Skills-Card eingetragen (skill = Fähigkeit, Können). Sind die Prüfungen zu den sieben Modulen erfolgreich abgelegt, wird der ›Europäische Computer Führerschein‹ ausgehändigt. Als ›Light‹-Version dieses Zertifikats gibt es noch den ›ECDL-Start‹, der aus wahlweise vier der angegebenen sieben Lerneinheiten besteht. Für den späteren Erwerb des kompletten ECDL haben diese vier Teilbereiche Gültigkeit.

Computer Führerschein – eine gute Idee!?

Im Prinzip ist ein solcher ›Computer-Führerschein‹ eine hervorragende Idee, kann er doch die in vielen Stellenausschreibungen geforderten PC-Kenntnisse greifbar machen und liefert erstmals ein europaweit standardisiertes Instrumentarium zum Erwerb solcher (Grund-)Kenntnisse.

Er kann damit auch ein wesentlicher Baustein sein für die so genannte ›Employability‹, also die Beschäftigungsfähigkeit von Arbeitnehmern und Arbeitnehmerinnen, die mit dem ECDL über die unmittelbare Berufsbildung hinaus heute unabdingbares Compter-Querschnittswissen erwerben können (siehe: ›Fit am Computer – Europäischer Computer-Führerschein‹ in cf 10/01 ab Seite 14).

Allerdings gibt es auch Kritik am ›Lappen für den Computer‹. Zu platt seien die Anforderungen, die Kurse zu teuer. So bezeichnete in einem Zeitungsartikel (›PC-Nutzer, Klasse Drei‹ in der SZ vom 4. 8. 2001) Eicke Lenz, der als ›Europa-Berater‹ des Arbeitsamts München ›mobilitätswilligen Arbeitnehmern‹ Auskünfte gibt, den ECDL als »Geldschneiderei hoch fünf« und rät, doch besser den PC-Führerschein des Arbeitsamts zu erwerben. Die ECDL-Kosten stünden in keinem Verhältnis zum Ertrag. »Wir bezahlen das nicht«, meint auch sein Kollege Peter Pauli, Bereichsleiter für die Überprüfung beruflicher Weiterbildungsmaßnahmen. Denn der ECDL vermittle »keine profunde Tiefe«, sondern höchstens »Standardwissen, das bald jeder Grundschüler haben wird«.

Wie steht's mit der ›profunden Tiefe‹?

Hier soll dem Kritikpunkt der ›profunden Tiefe‹ mal etwas Futter gegeben werden und zwar am Beispiel Datensicherheit und Datenschutz. Und zumindest dafür gilt:

Im Bereich Datenschutz und Datensicherheit erreicht der ECDL noch nicht einmal das Niveau des Standardwissens!

Bleiben wir dafür mal beim Bild der Fahrlizenz und stellen uns einen Autoführerschein vor, in dem zwar die Fahrzeugbedienung und die Verkehrsregeln vermittelt werden, aber keine Kenntnisse über die Gefahren bei Aquaplaning, Glatteis, nassen Blättern im Herbst, Ölspuren, Gefällstrecken und anderen Widrigkeiten. Genau das jedoch scheint beim ECDL der Fall zu sein: Im ganzen ECDL-Buch…[1] waren gerade einmal zwei (!) Stellen zu finden, an denen das Thema Datenschutz und Datensicherheit angesprochen wurden.

1… Wir beziehen uns auf: Munnely, Brendan und Paul Holden, ECDL / Der Europäische Computer Führerschein / Das komplette Kursbuch; Markt & Technik, 608 Seiten und eine CD-ROM, ISBN 3-8272-6034-5

Nicht einmal Grundlagenwissen

So gibt es im Modul 1 ›Grundlagen der Informationstechnik‹ einen Abschnitt zu ›Datenpflege – Sicherheit und Passwörter‹. Dort finden sich einige allgemeine Bemerkungen über Passwörter und noch ein paar Informationen über deren Zusammensetzung. Empfehlungen aber zum Aufbau und zum Wechselturnus der Passwörter und Informationen zu den verschiedenen Systemebenen (Betriebssystem, Netzwerk, Internet, Einzelprogramme) fehlen. Es folgen nur noch ein paar – allerdings weitgehend unbrauchbare – Ratschläge zum Thema Viren, Trojaner ⇨ und so weiter.…[2]

Im gleichen Modul findet sich dann zwar noch jeweils ein Abschnitt zu ›Datenschutz‹ und zur ›EU-Richtlinie zum Datenschutz‹: Aber auch hier sind es nur ein paar allgemeine Bemerkungen, Praktisches oder gar Handhabbares ergibt sich nicht.

Im Gegenteil: Chancen, den Datenschutz und die Datensicherheit an geeigneten Stellen zu thematisieren, werden gleich mehrmals vertan:

Im Modul 2 ›Computernutzung und Dateiverwaltung‹ wird anhand der Übung 2.31 erläutert, wie ein Bildschirmschoner eingerichtet oder geändert werden kann. Erwähnt wird, dass ein Bildschirmschoner heute nur noch dekorativen Zwecken diene, aber es gibt keine Bemerkung zu der Möglichkeit, einen Bildschirmschoner mit einem Passwort abzusichern und ihn damit für den sicheren Umgang mit Daten nutzbar zu machen … Das geht sogar so weit, dass zwar das Menü zur Einrichtung eines Bildschirmschoners abgebildet ist und die zu verrichtenden Arbeiten erläutert werden, das deutlich sichtbare Kontrollfeld ›Kennwortschutz‹ aber unerwähnt bleibt.

Im Modul 7 ›Informations- und Kommunikationsnetze‹ wird unter der Überschrift ›Massen-E-Mail und BCC‹ lediglich erläutert, der Sinn der ›Blind-Carbon-Copy‹-Funktion sei es, zu verhindern, dass eventuell einem Konkurrenten die E-Mail mit allen Adressen in die Hände fallen könne. Da ist sogar die für Kinder gedachte Website **blinde-kuh.de** in ihren Ratschläge deutlich konkreter und weitergehend – dort steht nämlich: »Und ganz wichtig, schütze die Daten anderer Kinder. Leite keine Kettenbriefe weiter und veröffentliche nicht deren Mailadressen auf deiner Homepage.« Und was ist es anderes, seinen kompletten Geschäftspartner-, Kunden- oder Kollegenkreis über ein Massen-E-Mail in die (Internet-)Welt hinauszuposaunen, nur weil man die BCC-Funktion nicht nutzt (siehe auch ›Informationsflut am Arbeitsplatz‹ in cf 4/03 ab Seite 26)?

Kurz und gut: Von einem ›Computer-Führerschein‹ muss deutlich mehr Substanz in Datenschutz- und Datensicherheitsfragen erwartet werden. Klar: So ein allgemeiner Schulungsleitfaden kann keine spezielle Datenschutz- und/oder Datensicherheitsschulung ersetzen und kann auch nicht so ganz nebenbei aus einem schlichten PC-Benutzer einen Datenschutzspezialisten machen. Das wäre ein überzogener Anspruch, das kann nicht die Zielsetzung eines Zertifikats sein, das nur Standardwissen vermitteln soll. Aber zu dem ›unabdingbaren Querschnittswissen für die PC-Benutzung‹ sollten doch einige Datenschutz-/Datensicherheits-Elemente mehr gehören als sie aktuell im ECDL enthalten sind.

Computer Führerschein – eine gute Idee!?

Wichtig wäre es vor allem, dabei nicht mit abstrakten Gesetzen und erhobenem Zeigefinger zu operieren, sondern behutsam aber deutlich die Sensibilität für dieses Gebiet zu fördern und beispielhaft Kenntnisse über Gefährdungen und ihre Vermeidung einfließen zu lassen. Dies könnte am besten durch unmittelbare Betroffenheit erreicht werden – durch Informationen wie diese zum Beispiel:

> ***»Ein Viertel der größeren US-amerikanischen Firmen hat bereits einmal einen Mitarbeiter wegen Missbrauch von Internet oder E-Mail gefeuert. Wie eine aktuelle Untersuchung der American Management Association, der nach eigenen Angaben weltweit führenden Ausbildungsorganisation für Management-Nachwuchs ergeben hat, kontrollieren inzwischen rund 80 Prozent der großen und mittelgroßen US-Firmen ihre Angestellten regelmäßig oder stichprobenartig bei der Nutzung von Internet, E-Mail oder Voice-Mail oder überwachen Mitarbeiter per Videokamera. Vor vier Jahren waren es gerade einmal 35 Prozent der Firmen, die zu solchen Mitteln griffen.« (aus: Telepolis von Heise)***

Oder:

> ***»Zwischen 81 und 86 Prozent aller Sicherheitsprobleme in der IT beruhen auf Irrtum und Nachlässigkeit.« (Wirtschaftswoche)***

Und ganz konkret gälte es, bei den Kursteilnehmern ein Gefühl dafür zu erzeugen, welche Gefährdungen für sie und andere mit der PC-Nutzung verbunden sind.

2… Zum Vergleich das, was zumindest die amtlichen Datenschützer empfehlen: www.lfd.m-v.de/informat/pwd/oh_pwd.html

Was unbedingt sein müsste ...

Hier einige – wenige – Beispiele, wie ganz konkret an den ohnehin behandelten Programmen für ein wenig Sensibilität gesorgt werden könnte…[3]:

Beispielbereich Betriebssystem Windows:

Gehen Sie mal auf *Start → Dokumente* und schauen Sie dort nach, welche Dokumente an Ihrem PC zuletzt aufgerufen wurden (möglich übrigens auch in Winword, Excel, Powerpoint usw.)

Falls sie in einem Netzwerk arbeiten, ist es sehr wahrscheinlich, dass Anmelde-/Abmelde-Zeiten gespeichert werden, ebenso wie Dateizugriffe und -speicherungen und weitere zuvor vom Systemverwalter definierte Ereignisse wie das Drucken übers Netzwerk oder Fehlzugriffsversuche protokolliert werden.

Beispielbereich Winword und Excel:

Schauen Sie doch mal unter ›Eigenschaften‹ eines Dokuments nach, was da alles so drinsteht über Sie und Ihren Umgang mit dem Dokument (siehe dazu auch: ›Was Word so alles verrät …‹ in CF 1/00 ab Seite 29).

Bedenken Sie dies, wenn Sie zum Beispiel Dokumente von anderen als Vorlage übernehmen und als Ihre eigenen Dokumente versenden – denn wenn Sie die Informationen nicht löschen oder überschreiben, bleiben sie in ›Ihrem‹ Dokument erhalten.

Oder wenn Sie die Funktion ›Schnellspeicherung zulassen‹ unter *Extra → Optionen → Speichern* aktiviert haben, dann sollten Sie vor dem Versand des Dokuments auf jeden Fall neu speichern (*Datei → Speichern unter …*). Bei Schnellspeicherung wird nämlich nur die Änderung zum vorherigen Zustand abgespeichert, der Empfänger sieht dann zwar auf den ersten Blick nur das gewollte Ergebnis, kann mit Einsatz eines entsprechenden ›Werkzeugs‹ aber ohne Weiteres sehen, welche Änderungen Sie bei der Texterstellung alle so vorgenommen haben. Das kann nicht nur dann peinlich werden, wenn man einen Brandbrief nach einem ›Drüber-geschlafen-haben‹ doch noch einmal entschärft hatte.

Oder Sie schützen Ihre Dokumente über die programmeigene Passwortfunktion in Winword oder Excel? Nun, dann sollten Sie bedenken, dass es im Internet eine Menge so genannter ›Passwortcracker‹ herunterzuladen gibt, die diesen Schutz sehr schnell ›knacken‹ können.

Beispielbereich E-Mail

E-Mails zu versenden, ist wie das Verschicken einer Postkarte: Beim Sender, unterwegs und beim Empfänger können sehr viele mitlesen … Insbesondere in Firmen gibt es ›Content-Security‹-Programme, die alle E-Mails aller Beschäftigten auf bestimmte verdächtige Inhalte hin abprüfen und im Falle des Falles automatische Meldungen an das ›Aufsichtspersonal‹ absetzen. Dabei kann es zum Beispiel um das Versenden von Geschäftsgeheimnissen, um unerwünschte gewerkschaftliche Aktivitäten oder um den Missbrauch von Firmeneinrichtungen gehen.

Und selbstverständlich kann immer nachvollzogen werden, an wen und von wem Sie E-Mails geschickt oder bekommen haben. Einige E-Mail-Programme speichern darüber hinaus auch Informationen zur weiteren Bearbeitung, also etwa ›gelesen am … / um …‹, ›weitergeleitet am … / um … / an …‹, ›gedruckt am … / um …‹ und so weiter.

Beispielbereich Internet

Sie hinterlassen Spuren zum Beispiel im Zwischenspeicher Ihres Internet-Programms (Browser-Cache), über den jeder weitere Benutzer ihres Computers dann nachschauen kann, wo sie im Internet überall vorbeigeschaut haben.

Passwörter von geschützten Internet-Seiten sollten keinesfalls auf Ihrem Rechner gespeichert sein, sonst kann unter Umständen jeder von Ihrem Rechner aus auf diese Seiten zugreifen.

In vielen Firmen werden so genannte Proxy-Server eingesetzt. Auf diesen speziellen Rechnern werden Kopien angesteuerter Internet-Seiten abgelegt, um einen nochmaligen Zugriff zu beschleunigen. Zugleich ist damit aber auch genau protokolliert, wer diese Seite wann aufgerufen hat.

Beispielbereich Verhalten

Wissen Sie eigentlich, dass die Weitergabe eines Passworts in bestimmten Fällen eine (zum Teil sogar fristlose) Kündigung rechtfertigen kann? Dann sollten Sie lieber darauf verzichten, im Vertretungsfall Ihrer Kollegin Ihr Passwort anzuvertrauen …

Fazit

In einem Werk, das die Zielsetzung verfolgt, »umfassende Kenntnisse im Umgang mit dem Computer zu vermitteln«, sollten Datenschutz (Eigenschutz und Fremdschutz) sowie die Datensicherheit ausführlicher behandelt werden – zumindest Letzteres wird auch jeder Arbeitgeber begrüßen. Sollte es aber – aus welchen Gründen auch immer – nicht möglich sein, diese Themen in ausreichendem Umfang noch in den ECDL aufzunehmen, wäre zumindest zu diskutieren, einen entsprechenden Warnhinweis in die Lehrbücher aufzunehmen:

»Vorsicht, diese Lehr-Unterlagen zum Gebrauch von Personal Computern vermitteln keine ausreichenden Kenntnisse über Datenschutz und Datensicherheit, hierzu wenden Sie sich bitte an …«

Knut Hüneke, Diplom-Psychologe, Schwerpunkt Arbeits-, Betriebs- und Organisationspsychologie, lebt in Nannhofen bei München und arbeitet als freiberuflicher Organisationsberater; Kontakt: **k.hueneke@link-m.de**; **www.khueneke.link-m.de**; Roland Schäfer, Fachkraft für Datenschutz, lebt und arbeitet in Frankfurt/Main; Kontakt: **schaefer@datenschuetz.de**

[3]… Wir beziehen uns hier auf den Quasi-Standard der Microsoft-Programme. Inzwischen ist gibt es zwar die Möglichkeit, den ECDL nicht nur auf Basis von Microsoft-Produkten abzulegend, aber es ist nicht anzunehmen, dass der hier angesprochene Mangel dort berücksichtigt ist.

[→] Trojaner = Trojanisches Pferd = Bezeichnung für einen speziellen Typ von Computer-Schädlings-Programmen (Viren); das ›trojanische Pferd‹ versteckt seine schädigende Funktion hinter einem scheinbar nützlichen Zweck.