UIMCommunic@tion

08/2020

Ausgabe für Deutschland

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Erst denken, dann machen: Was vor dem Verkauf eines PC beachtet werden sollte

Die Bundeswehr ist erneut in die Schlagzeilen geraten. Nach mangelhafter Ausrüstung, rechtsextremistischer Umtriebe in einigen Kasernen und der Beraterаffäre im Verteidigungsministerium geht es diesmal um die Informationssicherheit. Über die Internetplattform ebay wurde ein Bundeswehr-Laptop für 90 Euro verkauft, der noch vertrauliche Daten enthielt. Konkret fand sich unter anderem eine Anleitung, wie man das Flugabwehrsystem Ozelot im Notfall zerstört, berichtet das Nachrichtenmagazin DER SPIEGEL. Bereits im Juli 2019 war ein Bundeswehr-Laptop mitsamt Bedienungsanleitung für den Raketenwerfer „Mars" in privaten Besitz eines Försters geraten. „Es zeigt sich, dass alle Unternehmen gefordert sind, wenn es um das Ausrangieren von PCs, Laptops oder anderer Hardware geht. Nur weil die Geräte betriebswirtschaftlich abgeschrieben sind, sind sie noch lange nicht wertlos", richtet Datenschutzfachmann Dr. Jörn Voßbein eindringliche Worte an kleine und große Unternehmen und Institutionen. Welche Möglichkeiten bestehen, um solche peinlichen oder schädigende Momente für das eigene Unternehmen zu verhindern?

Wer seinen gebrauchten PC oder sein Notebook verkaufen will, sollte das alte Gerät passend vorbereiten. Nur so landen persönliche oder unternehmensrelevante Daten nicht aus Versehen in fremden Händen. Auch dem neuen Besitzer werden Unannehmlichkeiten erspart.

Drei Möglichkeiten bestehen, um mit alter Hardware umzugehen:

1. weiter nutzen,
2. zerstören oder
3. verkaufen.

Bei einem Verkauf sollten ein paar Dinge beachtet werden, damit nicht der Bundeswehr-Fall eintritt und vertrauliche Daten in die Hände von Fremden gelangen. Das größte Risiko beim PC-Verkauf ist das Zurückbleiben von Daten, mit denen man eindeutig den bisherigen Besitzer identifizieren kann. Im ersten Schritt sollten wichtige Daten, die noch auf dem Altgerät vorhanden sind, gesichert werden. Erst wenn alle wichtigen Daten vom alten Gerät auf ein neues Gerät übertragen wurden, sollte die Hardware des alten platt gemacht werden.

Die nachhaltigste und sicherste Lösung ist die physikalische Zerstörung der Festplatte. Allerdings ist dies keine Option, wenn der PC oder Laptop verkauft werden soll. Die sicherste Methode ist daher eine Grundreinigung. Es sind viele Dienstprogramme erhältlich, die die Daten auf der Festplatte durch mehrfaches Überschreiben sicher löschen, damit sie vom neuen Besitzer nicht wiederhergestellt werden können.

„Dass sensible Daten in die Hände von Dritten geraten, weil die Festplatte nicht komplett und gründlich gereinigt wurde, darf nicht passieren und kann Unternehmen in Ihrer Existenz gefährden", betont UIMC-Geschäftsführer Dr. Jörn Voßbein. Es drohen Strafen, Meldungen an staatliche Stellen, Image-Schäden und sonstige Nachteile, wenn vertrauliche Daten beispielsweise an den Wettbewerber gehen. „Bei besonders sensiblen Daten sollte man auch stets prüfen, ob es der kleine Erlös durch den Verkauf wert ist, ein solches Risiko einzugehen. Wir empfehlen die physikalische Zerstörung der Datenträger. Mancher Systemadministrator freut sich vielleicht auch über die Möglichkeit, an einer unschuldigen Festplatte seine Frustration abzubauen," sagt Dr. Voßbein mit einem Augenzwinkern.

Hinzu kommen noch Probleme, wenn die Geräte nicht Eigentum des Unternehmens sind, sondern geleast wurden. Die gilt beispielsweise auch für Drucker oder Multifunktionsgeräte, da diese – was oft vergessen wird – mittlerweile auch große Festplatten verbaut haben. Diese dürfen zumeist nicht ausgebaut werden oder man hat keine Administrationsrechte, um Löschroutinen mit o. g. Dienstprogrammen zu starten. In diesem Fall muss dringend mit dem Leasinggeber eine gemeinsame Lösung gefunden werden, schließlich werden die Geräte oftmals bei einem weiteren Leasingnehmer weitergenutzt.

FAQ: Aktualisierung der Datenschutzfolgeabschätzung im eCollege!

Die EuGH hat ein Urteil zum Privacy Shield und den Standardvertragsklauseln verkündet (siehe UIMCommunication 07/2020). Wir haben dementsprechend die nötige Aktualisierung der Datenschutzfolgeabschätzung Office 365 im eCollege vorgenommen (zugangsbeschränkt; bitte kommen Sie auf uns zu).

UIMC Dr. Vossbein GmbH & Co KG, Otto-Hausmann-Ring 113, 42115 Wuppertal
Tel.: +49-202-946 7726 200, Fax: - 19, E-Mail: consultants@uimc.de, Internet: www.UIMC.de

Noch Fragen?
Treten Sie mit uns in einen Dialog ein!

UIMCommunic@tion

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Zertifizierung

Testierung

Auditierung

Happy Birthday: 20 Jahre UIMCert

Die UIMC-Gruppe begeht am heutigen Tagen ein großes Jubiläum: UIMCert, eines der führenden Unternehmen in der Zertifizierung von IT-Sicherheit und Datenschutz, wird 20 Jahre alt. Die Geschichte des Unternehmens ist auch eine Geschichte der Entwicklung der Normen und Prüfstandards im Bereich des Informationssicherheitsmanagements.

Am 03.08.2000 gründete Prof. Dr. Reinhard Voßbein, langjähriger Professor für Betriebswirtschaftslehre mit dem Schwerpunkt Wirtschaftsinformatik an der Universität Duisburg-Essen, die UIMCert als Schwesterunternehmen der UIMC mit dem Ziel, eine praxistaugliche Zertifizierung des IT-Sicherheitsmanagement voranzutreiben. Ein Jahr zuvor hatte das British Standards Institute die BS7799:1999 als Norm für die Einführung eines Informationssicherheitsmanagementsystems vorgestellt. Dies war nicht die erste Version der Norm, aber die erste, die auf internationales Gehör stieß und der Ursprung der heute relevanten Normenreihe ISO/IEC 2700x ist. UIMCert wurde bereits im November 2001 als Zertifizierungsstelle für die BS7799:1999 akkreditiert und noch im selben Monat wurde das erste Zertifikat an die ZEDA erteilt.

Die Akkreditierung wurde bei der Erneuerung im Jahr 2006, dann nach der Norm ISO 27001:2005, um den Prototypenschutz gemäß den Vorgaben des Verbandes der Automobilindustrie erweitert. Seither ist UIMCert durchgängig akkreditiert, die letzte Re-Akkreditierung fand im Jahr 2019 statt.

Neben der IT-Sicherheit war auch der Datenschutz von Beginn an ein Fachgebiet der UIMCert: Anfang 2002 wurde UIMCert als sachverständige Prüfstelle gemäß der Landesverordnung über ein Datenschutzaudit des Landes Schleswig-Holstein anerkannt, damals als erste Prüfstelle für die beiden Bereiche Recht und Technik. Und noch im selben Jahr konnte die Unabhängige Landesbehörde Schleswig-Holstein auf Basis eines von UIMCert erstellten Gutachtens das erste Datenschutz-Gütesiegel an die Firma AVZ verleihen. 2007 wurde ferner der ComNetMedia AG das erste Datenschutz-Gütesiegel nach dem UIMCert eigenen Prüfstandard PS101 erteilt.

Im selben Jahr wurde das Angebot um ein weiteres Fachgebiet erweitert: die Erstellung von Testaten gemäß den Standards des Instituts der Wirtschaftsprüfer (IDW). Die Standards bilden eine Grundlage für die Prüfung rechnungsrelevanter Software und IT-Systeme. Einerseits ermöglicht es die PS-880 zu kontrollieren, ob die Vorgaben des Handelsgesetzbuches, der Abgabenordnung und die Grundsätze ordnungsgemäßer Buchführung eingehalten werden, und andererseits kann die verwendete Software gemäß der IDW PS-330/331 auf ihre Sicherheit geprüft werden.

Heute bietet UIMCert ein umfangreiches Portfolio an: Neben der klassischen Auditierung gemäß den Normen der ISO 2700x-Familie sind im Bereich der Informationssicherheit auch Checkups möglich. Im Bereich des Datenschutzes bietet UIMCert Audits auf Basis aller anwendbaren Datenschutzgesetze an. Weiterhin sind Audits nach den Sicherheitsstandards des Instituts der Wirtschaftsprüfer (IDW) möglich. Schulung, Fort- und Weiterbildung komplettieren das Programm. Nach dem Tod des Firmengründers Prof. Dr. Reinhard Voßbein im Jahr 2011 führt heute Arlette Schilde-Stenzel die Geschäfte der UIMCert. Sie wird unterstützt durch den Zertifizierungsstellenleiter Dr. Gerhard Weck. Einen besonderen Stellenwert im Unternehmen genießt nach wie vor die Teilnahme an wissenschaftlichen Projekten und Studien.

Updates/Neue Unterlagen im Online-Formular-Center

- Verfahrensverzeichnis mit Risikobewertung (Berücksichtigung des EuGH zum Privacy Shield im Rahmen des Drittlandtransfers.)
- Merkblätter für die Fachbereiche
- Anpassung aller Dokumente (Änderung der Dateiformate: docx, xlsx) www.online-formular-center.eu

Bitte senden Sie mir neben den angekreuzten Themen weitere Informationen zu:

- ☐ Was vor dem Verkauf eines PC beachtet werden sollte
- ☐ Aktualisierung der Datenschutzfolgeabschätzung im eCollege!
- ☐ **Unser Tipp:** Bitte senden Sie mir zukünftig den UIMCommunic@tion-Info-Brief und regelmäßig weitere interessante Informationen per E-Mail zu!

E-Mail: _____ Unterschrift: _____

per Fax an (0202) 946 7726 9200 oder formlos per Mail an communication@uimc.de

Mehr Informationen, Hinweise und Tipps finden Sie hier: https://communication.UIMC.de