



Datensicherheit muss gelernt sein

Der *Chaos Computer Club Luxembourg* zeigt sich besorgt gegenüber der heiklen Situation im Sportministerium, bei der **48.670** private und medizinische Datensätze von Sportlern **ohne** größere Vorsichtsmaßnahmen im Netz abrufbar waren.

Legitimation solcher Datenbanken

Die sogenannte „Médico-Sportif“ Datenbank, die vom „Centre Informatique de l'Etat“ administriert wird, enthält 48.670 Datensätze. Jeder dieser Datensätze enthält privat und medizinische Informationen zu einer Person. Da ein Mitarbeiter eines „Centre Médico-Sportif“ die Zugangsdaten zu eben dieser Datenbank auf einem Post-It auf seinem Bildschirm stehen hatte, war es der Person die den Vorfall bei den Behörden gemeldet hat ein leichtes sich Zugang zu diesen Daten zu verschaffen.

Nun stellt sich die Frage was denn eine Datenbank dieser Größenordnung legitimiert, in der solch private personenbezogene Informationen gespeichert sind und wer eigentlich **legalen** Zugriff darauf hat. Um der Datensparsamkeit gerecht zu werden, wäre eine Reevaluation der momentan gespeicherten Daten nötig, um festzustellen welche denn nun absolut keine oder nur sehr geringe Relevanz in Bezug zum "Médico-Sportif" haben und diese dann auch anschließend zu löschen.

Integrität des Systems

Bei den Sicherheitsmaßnahmen die – für eine Datensammlung dieser Art – ergriffen worden sind, hat man fahrlässig gehandelt. Die Datenbank war nicht ausreichend vom Internet abgeschirmt und durch zwei simple Logins erreichbar. Ein solches System muss einen Zugriff von einem nicht autorisierten PC verhindern, beispielsweise durch „IP-Filtering“ oder besser durch ein geschlossenes VPN-Netzwerk. Dies einzurichten ist kein Hexenwerk und sollte die Administratoren nicht vor unlösbare Probleme stellen.

Der ausschlaggebende Angriffsvektor heißt allerdings: Mensch. Aufgrund mangelnder „Human Security Awareness“ wurde jedem die Möglichkeit gegeben sich die Login-Daten zu fotografieren, kopieren, etc. und anschließend die Datenbestände einzusehen. Identitätsfälschung, Mobbing, Kündigungen, etc. könnten direkte Konsequenzen dieser Datensätze sein, falls sie in die Hände der falschen Personen gelangen würden.

Konsequenzen für die Datensicherheit

Wer kann garantieren, dass nicht bereits andere unautorisierte Zugriffe auf dieses System stattgefunden haben oder gar bereits Daten entwendet wurden, **bevor** diese Person Zugriff auf das System hatte und es den zuständigen Stellen gemeldet hat?!

Ob nun Datensätze kopiert wurden oder nicht, kann nur die Person sagen die hinter der Enthüllung dieses Missstandes steckt. Allerdings bedauert der *Chaos Computer Club Luxembourg* es stark, dass nun versucht wird ein Exempel an dieser Person durch Anklage zu statuieren, anstatt zu einem Dialog aufzurufen - welcher auch vorerst anonym stattfinden könnte - und ohne direkt mit rechtlichen Konsequenzen zu drohen.

Es ist zu begrüßen, dass auf der gestrigen Pressekonferenz Justiz- und Kommunikationsminister François Biltgen betonte, dass in Zukunft weitere Maßnahmen zu Gunsten der Datensicherheit des Luxemburger Staates investiert werden, doch waren diese sehr wage gehalten und lässt einen zum Schluss kommen, ob es denn immer zu erst zu einem Vorfall kommen muss bis entsprechende situationsangepasste Massnahmen in die Wege geleitet werden?

Chaos Computer Club Luxembourg

(Presse)kontakt:

E-Mail: info@c3l.lu / press@c3l.lu

Tel.: +352-691-71-77-44

Webseite: <http://c3l.lu> / <http://c3l.lu/wiki/Medicoleak>