



Datenschutz- Newsletter

**Datenschutz bedeutet vernünftig
mit den Daten umzugehen die uns
überlassen wurden!**



© Bernd Schneider

Sehr geehrte Damen und Herren,

dieser Datenschutz-Newsletter soll zukünftig in unregelmäßigen Abständen erscheinen und Sie über Datenschutzthemen informieren, die uns alle angehen. Dabei brauchen wir auch Ihre Hilfe, schreiben Sie uns doch was Sie zum Thema Datenschutz interessiert und bewegt. Wir werden dann die Themen aufnehmen und in den nächsten Newslettern versuchen zu behandeln.

Ihr

Indra Sommerfeldt Eckhard Andree Claus-Christian Schneider-Pardun Bernhard Stengel

Fake Anrufe von Microsoft Mitarbeitern!

Inhalt

Fake Anrufe von Microsoft Mitarbeiter	1
Passwörter sind wie Zahnbürsten	2
Passwort weg - Ruf ruiniert	2
Passwörter ein gutes Geschäft für die Internetmafia	3
Regeln für sichere Passwörter	4
Passwörter kompliziert, komplex und doch einfach!	4
Weitere Informationen finden Sie in unseren FAQ auf der Datenschutzseite im Intranet!	

Vorsicht, Phishing! Betrügerische E-Mails erkennen



Gefälschte Absender-Adresse

Ist die E-Mail-Adresse des Absenders z.B. durch einen Vergleich zu verifizieren? Kann der Absender den Versand der Mail persönlich/telefonisch bestätigen?



Abfrage vertraulicher Daten

Fordert die E-Mail zur Eingabe persönlicher Informationen auf? Werden Geheimnummern oder Passwörter abgefragt?



Vorgetäuschter dringender Handlungsbedarf

Signalisiert die E-Mail Dringlichkeit oder Handlungsbedarf? Wird eine Nachricht des Absenders erwartet?



Links zu gefälschten Webseiten

Enthält die E-Mail Verlinkungen, die auf andere Webseiten verweisen? Welche Ziel-URL wird bei einem Mouseover angezeigt?



Sprachliche Ungenauigkeiten

Ist die Anrede unpersönlich formuliert? Enthält der Text Rechtschreib- oder Zeichenfehler?



In der letzten Zeit gibt es häufig Anrufe von Kriminellen die sich als Mitarbeiter von Microsoft ausgeben.

In manchen Fällen versuchen diese Menschen Informationen von Ihnen zu erlangen, sogenanntes Phishing und es gibt Anrufe, bei denen die Kriminellen von Ihnen verlangen eine Software für einen Fernzugriff oder als Fehlerkorrektur zu installieren.

Dadurch erhalten dann die Kriminellen vollen Zugriff auf ihre und/oder unsere IT und können Daten klauen, zerstören und Schadsoftware installieren.

Beachten Sie, Mitarbeiter von Microsoft werden Sie niemals direkt kontaktieren!

Wenn, dann wird die IT-Abteilung kontaktiert! Verweisen Sie immer auf die O-IT oder die IT-Abteilung der Regionalverwaltungen! Wenn es tatsächlich ein Problem geben sollte, wissen die was zu tun ist!

Bitte geben Sie niemals Passwörter oder Zugangsdaten an Dritte weiter oder installieren Sie Software ohne Rücksprache mit O-IT oder der IT-Abteilung ihrer Regionalverwaltung!

Passwörter sind wie Zahnbürsten!



Pixabay

Na, können Sie es sich denken wieso?

Was passiert, wenn Sie Ihren Benutzer und Ihr Passwort mit jemanden anderen teilen? Der andere kann alles sehen, was auch Sie sehen, auch wenn er die Informationen eigentlich nicht sehen sollte!

Alles was er macht, wird so protokolliert, als wären Sie es gewesen. Wenn er also etwas falsch macht, ist es so, als wenn Sie etwas falsch gemacht haben.

Deshalb halten Sie es bei Ihren Passwörtern immer wie bei Ihrer Zahnbürste, teilen Sie diese niemals mit jemand anderem! Wenn es wirklich nicht anders geht, ändern Sie das Passwort danach sofort. Das Passwort ist dann natürlich auch für die Zukunft verbrannt und kann nicht mehr genutzt werden!

Passwort weg – Ruf ruiniert!



Pixabay

Die folgende Geschichte ist wirklich passiert und kann jedem von uns passieren!

Ein Familienvater hatte bei E-Bay ein Konto. Hacker hatten sein Passwort in Erfahrung gebracht und kurzerhand das Konto übernommen und das Bankkonto geändert. Dann haben sie in E-Bay eingestellt, dass Sie einen Posten sehr günstiger Tablets zu einem extrem günstigen Preis von 50 € pro Tablet zu verkaufen hätten. Eine große Anzahl von E-Bay-Kunden kauften ein oder mehrere Geräte und überwiesen den Kaufpreis auf das angegebene Bankkonto. Die Tablets wurden allerdings niemals geliefert.

Was passierte dann?

Eines Morgens stand die Polizei vor der Tür und holte alle Rechner ab, da sich die geprellten Kunden bei E-Bay beschwert hatten. Die Nachbarn haben dies natürlich mitbekommen und die wildesten Gerüchte breiteten sich aus. Angefangen von Internetbetrug, über Drogenhandel und Verbreitung von Kinderpornographie.

Die Polizei ermittelte natürlich sehr schnell, dass der Familienvater nichts mit dem E-Bay Betrug zu tun hatte und selbst geschädigter war, deshalb bekam er schnell seine Rechner zurück und es wurde auch keine Anklage gegen ihn erhoben. Dies bekam die Nachbarschaft natürlich nicht mit.

Dennoch bekam er danach Mahnungen von den geprellten Kunden und es dauerte nicht lange, da standen auch schon Inkassounternehmen vor der Tür, darunter auch Moskauer-Inkasso, die auch rechtlich eher bedenkliche Maßnahmen androhten, sollte das Geld nicht gezahlt werden.

Am Ende der Geschichte musste die Familie umziehen, da im Ort die wildesten Gerüchte über sie verbreitet wurden und immer wieder Inkassounternehmen der übelsten Sorte auftauchten.

Passwörter ein gutes Geschäft für die Internetmafia



Pixabay

Passwörter sind viel Wert für Kriminelle. So gibt es in China eine Gruppe, die nichts anderes macht als zu versuchen Passwörter von Benutzern herauszufinden. Wenn Sie diese haben, werden die Benutzernamen und Passwörter an andere Internetkriminelle verkauft.

Aber wie läuft das ab?

In vielen Fällen gibt es bei Online-Shops Programmierfehler. Die Angreifer können dann im Feld, in dem der Benutzername eingegeben wird einen Datenbankbefehl eingeben (SQL-Injektion) und dann wird die Liste aller Benutzer und deren Passwörter ausgegeben.

Im zweiten Schritt wird dann die Liste in eine Software eingelesen, die im Internet frei verfügbar ist und von jedem heruntergeladen werden kann. Diese prüft dann ob der Benutzer und das Passwort auch bei anderen Internetseiten wie z.B. Amazon, E-Bay ... funktioniert. Die Liste der Benutzer und Passwörter, sowie der Internetseiten bei denen diese funktionieren werden dann weiterverkauft und später für Internetbetrug genutzt.

Aus diesem Grund ist es sehr wichtig, dass Sie niemals ein Passwort mehrfach verwenden!

Später zeigen wir Ihnen, wie Sie dennoch relativ einfach Passwörter generieren können, die sich unterscheiden, die Sie sich aber dennoch gut merken können.


Sie möchten wissen ob eines Ihrer Passwörter gehackt wurde? <https://sec.hpi.de/ilc/search?lang=de>

Nutzerkonten	Leaks	Geleakte A
12.762.125.633	1.444	1.6

Wurden Ihre Identitätsdaten ausspioniert?

Täglich werden persönliche Identitätsdaten durch kriminelle Cyberangriffe erbeutet. Ein Großteil dieser Daten wird anschließend in Internet-Datenbanken veröffentlicht und dient als Grundlage für illegale Handlungen.

Mit dem HPI Identity Leak Checker können Sie mithilfe Ihrer E-Mailadresse prüfen, ob Ihre persönlichen Daten bereits im Internet veröffentlicht wurden. Per Datenabgleich wird kontrolliert, ob Ihre E-Mailadresse mit anderen persönlichen Daten (z.B. Telefonnummer, Geburtsdatum oder Adresse) im Internet verknüpft werden könnte.

 Bitte geben Sie hier Ihre E-Mail-Adresse ein.

Die von Ihnen eingegebene E-Mail-Adresse wird lediglich zur Suche in unserer Datenbank verwendet. Versenden einer Benachrichtigungs-E-Mail benutzt. Sie wird von uns in verschleierter Form gespeichert.

Hasso Plattner Institut

Regeln für sichere Passwörter!



Top 30 Most Used Passwords in the World		
1	123456	princess
2	password	letmein
3	123456789	654321
4	12345	monkey
5	12345678	27653
6	qwerty	1qaz2wsx
7	1234567	123321
8	111111	qwertyuiop
9	1234567890	superman
10	123123	asdfghjkl
11	abc123	
12	1234	
13	password1	
14	iloveyou	
15	1q2w3e4r	
16	000000	
17	qwerty123	
18	zaq12wsx	
19	dragon	
20	sunshine	

lightonconspiracies.com Free Content

1. Benutzen Sie niemals Passwörter, die Sie im privaten Bereich nutzen auch bei der Arbeit!

Im Internet besteht immer das Risiko, dass ein Passwort gestohlen wird. Wird dies Passwort auch im Unternehmen genutzt, dann sind auch die Daten im Unternehmen in Gefahr! Hacker wissen, dass Mitarbeiter oft die gleichen Passwörter privat nutzen, die sie auch im Unternehmen nutzen. Es ist oft leicht für sie herauszufinden wo und als was man arbeitet. (z.B. über XING, LINKEDIN, ...)

2. Nutzen Sie Passwörter, die mindestens 8 Zeichen lang sind. Je kürzer ein Passwort ist, desto schneller kann es gehackt werden. Ein Passwort mit sechs Zeichen kann man mit der richtigen Software innerhalb von 10 Minuten knacken. Bei 8 Zeichen dauert dies schon Wochen oder Monate. Wer lebt wohl gefährlicher jemand, bei dem ich das Passwort innerhalb von 10 Minuten hacken kann oder jemand bei dem ich Wochen oder Monate brauche. Auch bei Hackern ist Zeit Geld!
3. Verwenden Sie keine Wörter aus dem Wörterbuch, denn die Hackersoftware nutzt Wörterbücher um Passwörter zu knacken.
4. Als letztes, machen Sie es den Angreifern noch schwerer und verwenden Sie mindestens ein Sonderzeichen und Zahlen.

Passwörter kompliziert, komplex und doch einfach!

Maximale Rechenzeit eines Brute-Force-Angriffs bei einer Milliarde Schlüsseln pro Sekunde

Zahl und Art verwendeter Zeichen (Zeichenraum)	Passwortlänge 4 Zeichen	6 Zeichen	8 Zeichen	10 Zeichen	12 Zeichen
10 [0-9]	🔒 unter 1 ms	🔒 unter 1 ms	🔒 100 ms	🔒 10 Sek.	🔒 17 Min.
26 [a-z]	🔒 unter 1 Sek.	🔒 unter 1 Sek.	🔒 4 Min.	🔒 2 Tage	🔒 3 Jahre
52 [a-z + A-Z]	🔒 unter 1 Sek.	🔒 20 Sek.	🔒 15 Stunden	🔒 5 Jahre	🔒 12.400 Jahre
62 [a-z + A-Z + 0-9]	🔒 unter 1 Sek.	🔒 58 Sek.	🔒 3 Tage	🔒 27 Jahre	🔒 102.000 Jahre
96 (alles plus Sonderzeichen)	🔒 unter 1 Sek.	🔒 13 Min.	🔒 84 Tage	🔒 2108 Jahre	🔒 19 Mio. Jahre

Daten: Wikipedia
Legende: 🔒 sehr sicher | 🔒 einigermaßen sicher | 🔒 nicht sicher

Wikipedia

Also ehrlich, ich kann gut verstehen, wenn Sie jetzt denken, der hat doch einen Knall! Lange, komplexe Passwörter, die keine Wörter aus dem Wörterbuch sein sollten und dann auch noch für jeden Zugang ein anderes? Wer soll damit denn zurechtkommen!

Na schauen wir doch mal.

Es gibt verschiedenste Methoden um relativ einfach eine Menge komplexer unterschiedlicher Passwörter zu

generieren, die man sich auch merken kann. Ich nutze dazu die folgende Methode!
Jeder von Ihnen kennt Liedertexte, Gedichte oder Sprüche. Ich bin zum Beispiel ein Fan von den Beatles. Ja ich gebe zu ich bin nicht mehr der Jüngste! Viele kennen noch das Lied: "All You Need is Love" Um ein Passwort zu generieren habe ich einfach jeweils die ersten beiden Buchstaben der Worte genommen

All You Need is Love = alyoneislo

Oder wie wäre es mit einem Gedicht:

Die Glocke von Schiller (da der Satz länger ist habe ich nur jeweils den ersten Buchstaben genommen, man kann jedoch auch immer die ersten beiden nehmen. Ist dann sicherer, da das Passwort länger ist.

Fest gemauert in der Erden steht die Form aus Lehm gebrannt = fgidesdfalg

Wer noch besser sein will kann z.B. O durch eine = 0 oder ein i durch eine 1 ersetzen. Man sollte jedoch immer die gleichen Regeln nutzen.

Natürlich kann man auch über einfache Sätze die man sich merken kann ein Passwort generieren:

Mein Auto muss im Dezember in die Inspektion! = meaumimdeindiin

So nun haben wir ein Passwort, aber brauchen wir wirklich für jeden Zugang ein ganz neues Passwort? Wir hatten ja gesehen, dass Hacker prüfen ob man bei verschiedenen Zugängen dasselbe Passwort benutzt hat. Dabei prüfen Sie jedoch immer auf genaue Übereinstimmung.

Deshalb ergänzen wir einfach das Passwort bei jedem Zugang. Man muss sich dabei nur eine Regel ausdenken, die man immer nutzt.

Also stellen wir uns vor, wir haben Konten bei Amazon, Yahoo, e-Buy, EKHN.

Eine Möglichkeit ist z.B. das man immer die letzten drei Buchstaben der Anbieter nimmt.

Amazon --> zon dies hängt man dann an das Passwort an oder stellt es davor, am besten in Verbindung mit Sonderzeichen z.B. !zon!

Unser Satz: All You Need is Love

Amazon= !zon!alyoneislo oder alyoneislo?zon?

Yahoo= !hoo!alyoneislo oder alyoneislo?hoo?

e-buy= !buy!alyoneislo oder alyoneislo?buy?

EKHN= !look!alyoneislo oder alyoneislo?KHN?

Bei den ersten malen, wenn Sie die neuen Regeln und Passwörter nutzen merken Sie, dass es noch ungewohnt ist, aber glauben Sie mir, sie gewöhnen sich schnell dran und dann ist es Kinderleicht, solange Sie sich ihre Regeln merken. Wichtig ist auch, geben Sie die Regeln, wie Sie Ihr Passwort aufbauen nicht an Dritte weiter.

Impressum:

Herausgeber: Datenschutzabteilung der EKHN

Paulusplatz 1, 64285 Darmstadt

Tel.: 06151 405 303, Mail: Datenschutz@ekhn.de

Verantwortlich für den Inhalt:

Claus-Christian Schneider-Pardun

Eckhard Andree