Mag. Novotny: Praxistipps zum Gefahrenherd Browser.

Teil 2 von „Schwachstelle Mensch und Handlungsbedarf aufgrund DSGVO!

Seit Monaten ist die Umsetzung der Datenschutzgrundverordnung DSGVO in aller Munde. Und ebenso oft kann man über **Hacker-Angriffe und Erpressungsversuche** lesen. Ein verschlüsselter Computer oder das gesamte Netzwerk werden erst freigegeben, wenn man Lösegeld bezahlt.

Die Corona-Pandemie und das **verstärkte Arbeiten im Home-Office** bei gleichzeitig starkem Trend zur Digitalisierung haben unserer Wahrnehmung nach das Problem noch größer werden lassen. Daher hatten wir im **Teil 1** dieser Serie auf eine **überaus nützliche Homepage und deren Newsletter-Service hingewiesen.** Deren Ziel ist es, auf Betrugsmaschen, Fallen und Fakes im Internet hinzuweisen, um Problembewusstsein zu schaffen und im Idealfall zu helfen, dass man darauf nicht reinfällt. **Zum Nachlesen** hier klicken…

Was hat ein Hacker-Angriff mit der DSGVO zu tun?

Unser heutiger Praxistipp wird nicht nur hilfreich sein, sondern könnte für Unternehmen womöglich **„überlebenswichtig"** werden. Denn Hacker-Angriffe können eine Verletzung der DSGVO-Pflichten aufzeigen und damit zu Image-Verlust bei Kunden, aber auch zu Haftungsfolgen (wenn mit den gestohlenen Daten etwas passiert), und möglicherweise auch zu einer Bestrafung aufgrund der DSGVO führen.

Warum?
Aufgrund der DSGVO sind Sie verpflichtet, die Daten Ihrer Kunden, Partner, etc. sicher zu speichern und zu verarbeiten. Und um das **zu gewährleisten, müssen Sie TOMs einführen** und im Betrieb umsetzen. **Und regelmäßig überprüfen und bei Bedarf auch aktualisieren.**

Zum Erinnern: Was sind TOMs?
TOM ist die Abkürzung für „**T**echnische und **O**rganisatorische **M**aßnahmen".

Diese technischen und organisatorischen Maßnahmen, die Sie im Unternehmen setzen müssen, werden im **Artikel 32 der DSGVO definiert.** Sowohl **Verantwortliche, aber auch Auftragsverarbeiter** haben dafür zu sorgen, dass „geeignete technische und organisatorische Maßnahmen" implementiert sind, die sicherstellen, dass „ein angemessenes Schutzniveau gewährleistet ist".

Diese TOMs sollen sicherstellen, dass die **Vertraulichkeit, Integrität, Verfügbarkeit und Sicherheit** der Daten und damit der Systeme gegeben sind. Für den Verantwortlichen sind dabei der **Stand der Technik**, die Implementierungskosten und das **Risiko** (Eintrittswahrscheinlichkeit und Schadenshöhe) **zu berücksichtigen.**

Weitere Details zu den einzelnen TOMS haben wir in zwei Beiträgen im Vorjahr erläutert.
Zum Nachlesen: TOMs Teil 1 mit Zutritts-, Zugangs-, Zugriffs- und Weitergabe-Kontrolle. Hier…
Zum Nachlesen: TOMs Teil 2 mit Eingabe-, Auftrags-, Verfügbarkeits- und Datentrennungskontrolle. Hier…

Den heutigen **2. Teil** der Serie haben wir mit „Gefahrenherd Browser" bezeichnet. Denn der **Browser ist nicht nur das Tor ins Internet,** sondern laut Computerzeitung Chip.de das am häufigsten genutzte Programm am PC und „stehe damit ganz vorne in der Schusslinie für Angriffe".

In unserem heutigen Praxis-Tipp sehen wir uns an, **welche Browser wie anfällig sind** und wie man durch selbstgewählte Einstellungen einigen Gefahren die **Giftzähne ziehen** kann.

Hitliste der Sicherheitslücken 2022 (Quelle Chip.de):

1. Chrome: 303 Schwachstellen, 2. **Firefox:** 117, 3. **Edge:** 103, 4. **Safari:** 26 Schwachstellen.

Auch die **Statistik der letzten 20 Jahre** führt **Googles Chrome (3.159)** an, dann folgt Firefox mit 2.361 Lücken. Dahinter rangieren Internet Explorer (1.828), Safari (1.139) und Edge (828).

Zurecht verweist Chip in der Analyse darauf, dass man aus der bloßen Zahl der Sicherheitslücken nicht zwangsläufig auf das **Gefährdungs-Potential rückschließen** kann. Aber obige Statistik zeigt deutlich, dass Browser ganz oben auf der Hacker-Liste stehen. Ja, Sicherheits-Lücken werden immer wieder gefunden und durch Sicherheits-Updates beseitigt. Aber solange die Lücke offen ist, kann man sicher sein, dass Hacker diese nutzen, um in die Systeme einzudringen.

Denn es gibt einen florierenden Markt: **Hacker kaufen das Wissen um Lücken und die Tools**, um diese zum Hacken zu verwenden im Internet ein. **EDV- und Datenschutz-Experte Erich von Maurnböck** nannte kürzlich im AFPA-Webinar konkrete Zahlen:
Ransomware (braucht man zum Verschlüsseln von PCs) kostet 60 € oder 30% vom „Erlös des Hacks. Exploits Kits (Baukästen für Malware, also Schadsoftware) kosten ca. 1.400 €. Denial of Service-Tools kosten 800 €. Also überschaubare Kosten für Hacker, enormes Bedrohungs- und Schadenspotential für uns alle. Zero-Day-Exploits (das Wissen über noch nicht bekannte Sicherheitslücken), kosten rund 50.000 Euro, aber dafür gibt es eine **Lücke, gegen die niemand geschützt ist…**

Was sollte man tun? Standard-Einstellungen ändern und Add Ons nutzen
Keine Software ist perfekt, Sicherheitslücken gibt es überall. Aber man kann einige **Einstellungen im Browser** setzen, um die Sicherheit im Netz zu erhöhen und weniger Spuren im Netz zu hinterlassen. Und man kann den Browser durch ergänzende Software-Tools (Add Ons) erweitern. Allerdings sollte man hier auf geprüfte Software und Empfehlungen von sicheren Quellen achten.

Da Chrome und Firefox besonders viele Lücken haben, weisen wir auf nützliche **Erweiterungs-Empfehlungen** für diese beiden Browser hin. Wobei hervorzuheben ist, dass Firefox bewusst mehr Wert auf **Daten-Sicherheit und Datenschutz** legt. Und sich da von Datenkraken unterscheidet.

a) Standard-Einstellungen des Browsers ändern
Das Computer-Magazin PCtipp hat nützliche Hinweise für die Browser Crome, Firefox und Edge zusammengetragen, die ohne Fachkenntnisse und mit wenig Aufwand die Risiken bei Browser-Aktivitäten minimieren können. Diese Tipps geben wir hier als Anregung verkürzt wieder. Und ergänzen diese mit eigenen Tipps.
Wenn Sie den **gesamten Beitrag samt Screenshots** zum besseren Auffinden der konkreten Einstellung nachlesen möchten, bitte hier klicken…

Vorausgeschickt sei: Die **Standard-Einstellungen werden oft aus Bequemlichkeit nicht geändert.** Auch, weil man nicht weiß, welche Gefahrenpotentiale sich hier verbergen.
Dieses sorglose Akzeptieren erleichtert jedoch das Sammeln von Daten über Ihre Interessen, aber auch das „Phishen" von Daten zum Zwecke von Lösegeld-Forderungen, etc.

a1) Automatische Updates einstellen
Browser werden alle paar Wochen aktualisiert. Wie bei jeder Software gilt, dass auch jene des Browsers aktuell bleiben muss, um neu gefundene Sicherheitslücken geschlossen zu halten. Das ist auch eine Pflicht aus der DSGVO (siehe oben).

a2a) Daten nach Session löschen, **keine Chronik** anlegen lassen
In den Einstellungen gibt es unter dem Punkt Datenschutz und Sicherheit die Möglichkeit auszuwählen, dass Daten beim Schließen des Browsers gelöscht werden und auch keine (oder nur für ausgewählte Webseiten) eine Surf-Chronik angelegt werden darf.
Tipp: Bei Bank-Webseiten ist es meist nötig, dass Sie Cookies erlauben (also eine Ausnahme zulassen).

a2b) Incognito-surfen, Privater Modus
Was Sie unter a2a) händisch eingestellt haben, können Sie durch ein Hackerl bei Incognito bzw. Privater Modus ebenso erreichen. Dieser Modus bewirkt, dass der Browser die Cookies und Daten der besuchten Webseiten beim Beenden des Browsers löscht. Erkennbar im Firefox etwa durch eine **liegende Acht,** die wohl eine venezianische Augenmaske symbolisieren soll.

a3) Gefahrenquelle Pop-Ups und Adobe-Flash
Das sind die **zwei größten Einfallstore** für Schadsoftware. Daher empfehlen Datenschützer diese standardmäßig zu blocken bzw. zu verbieten.
Manche Seiten werden dann nicht „normal funktionieren". Wenn Sie das stört, können Sie dieses Pop-Up für eine vertrauenswürdige Seiten erlauben und diese Ausnahme abspeichern.

a4) Do-not-track-Funktion (Aktivitäten-Schutz)
Webseiten möchten gerne mitverfolgen, was alles Sie sich dort angesehen haben. Das können Sie abschalten. Die „Guten" werden Ihren Wunsch beherzigen.

a5) Warnung vor Add On-Installation einschalten
Sollte die besuchte Webseite versuchen ein Add on unbemerkt und ohne Ihre Zustimmung zu installieren, dann wird gewarnt. Und Sie können entscheiden, ob Sie das zulassen wollen oder nicht.

a6) Phishing- und Malware-Block-Funktion aktivieren
Diese Funktion gibt es zumindest im Firefox. Die Idee dahinter: Wenn man auf eine Phishing-Mail reingefallen ist und im Mail auf einen Link zu einer bösen Webseite anklicken möchte, kann diese Funktion verhindern, dass die Seite aufgeht (weil diese Webseite von anderen schon als verdächtig oder schädlich gemeldete wurde).

a7) Keine Passwörter, Kreditkarten und Formulareinträge speichern lassen
Ja, es ist bequem, aber hier sollte Vernunft über Bequemlichkeit siegen. Oder wollen Sie wirklich, dass z.B. Kreditkarte und Freigabe-Codes beim Online-Shopping im Browser gespeichert sind? Wenn die Passwörter zu viele werden, ist die sichere Variante ein Passwort-Manager!

a8) Standard-Suchmaschine ändern
Checken Sie in den Einstellungen welche Suchmaschine aktiv wird, wenn Sie im Suchfeld oder Befehlszeile etwas eintippen. Wenn Sie nicht Datenkraken Ihr Suchverhalten mitteilen möchten, können Sie andere Suchmaschinen nachladen und Ihre Wunsch-Suchmaschine mit einem Hackerl aktivieren und zur Standard-Suchmaschine machen.
2 Tipps dazu: **Ecosia** nutzt einen Großteil der Einnahmen dafür, um in Afrika Bäume zu pflanzen. Motto: Suchen und etwas Gutes für die Umwelt tun…
FirstPage nutzt die Google-Suche, anonymisiert aber die Suche und deren Ergebnisse, sodass Ihre Suchgewohnheiten bei Google nicht gespeichert werden können.

b) Erweiterungen / Add Ons für Browser

Wie schon oben berichtet: Wer mehr Sicherheit will, muss viele kleine Schritte setzen. Also die bequemen Standard-Einstellungen abändern.

Um die Sicherheit zu erhöhen, können Sie zusätzliche Add Ons nutzen. Achten Sie jedoch darauf, dass diese Empfehlungen von vertrauenswürdigen Seiten stammen und von sicheren Seiten heruntergeladen werden. Hier ein paar Tipps:

b1) VPN, Abkürzung für Virtual Private Network
Aus Sicherheitsgründen sollten Sie eine VPN-Software **für den gesamten PC nutzen,** denn damit schützen Sie online Ihre Privatsphäre. Sollten Sie so etwas noch nicht haben, laden Sie sich zumindest VPN-**Add-On für den Browser** herunter. **Es gibt kostenlose Tools, ob die aber wirklich und verlässlich tun, was sie sollen?**

b2) Ghostery entlarvt „Spione“
Dieses Add On zeigt an, **ob und welche Tracker** auf einer angesurften Webseite genutzt werden. Und man kann damit Werbung und Tracker blockieren. Was Ihre Sicherheit erhöht.
Achtung: Zahlreiche kostenlose Webseiten finanzieren sich durch Werbeeinnahmen. Wenn Sie solche Seiten unterstützen möchten, können Sie trotz Nutzung von Ghostery Werbung für solche Seiten gezielt erlauben. Man kann also das Tool – wenn man das will – je nach Website ein- und ausschalten.

b3) Firefox Multi-Account Containers
An einem PC vermischt sich oft Privates und Berufliches: Also neben beruflichem Surfen gibt es auch privates Surfen, Bankgeschäfte oder Shopping. All das wird – wenn Sie nicht unsere oben genannten Tipps anwenden – vermischt und ergibt ein sehr exaktes Bild von Ihrem Surfverhalten und Interessen. Dieses Container-Add On ermöglicht es die verschiedenen Bereiche in unterschiedliche „Schubladen“ abzulegen. Man erkennt sie an optisch anders eingefärbten Tabs. Unter der Haube trennt Firefox für die verschiedenen Container Cookies, Caches und temporäre Speicherbereiche auf. Also Cookies, die in einem Container heruntergeladen wurden, sind in anderen Containern nicht verfügbar. Auch Spuren von privat genutzten Social Media können nicht mit beruflichen Tracking Spuren kombiniert werden. Somit soll auch das Tracking über z.B. Facebook-Buttons und Pixels nicht mehr klappen.
Wie genau Sie bei der Installation vorgehen müssen, erfahren Sie auf der Mozilla-Hilfeseite hier…

b4) Fake-Shop-Detektor
Eine Entwicklung des Österreichischen Institut für angewandte Telekommunikation (ÖIAT) hilft zu erkennen, ob ein Angebot oder ein Shop nicht zu günstig, um wahr zu sein, ist.
Ja, eigentlich kennt man die Warnzeichen: Produkt gibt es sonst nirgends und ist sensationell günstig. Kein oder komisches Impressum. Nur Vorkasse erlaubt. Aber das Angebot ist halt so ein Schnäppchen. Und plumps, schon ist man doch reingefallen.

Dieses Add On hilft Fakeshops im Internet zu enttarnen!
Und zwar durch ein **zweistufiges Verfahren:** Einerseits wird die aufgerufene Webadressen mit einer Datenbank bereits bekannter Fake-Shops, aber auch vertrauenswürdiger Shops abgeglichen. Sollte es ein Fake-Shop sein, öffnet der Browser die Seite gar nicht sondern blendet die Warnung ein, dass man dort besser nicht einkaufen solle.

Wird die Webadresse in der Datenbank nicht gefunden, so wird mit Hilfe eines KI-Modells die Webseite anhand Tausender Merkmale in Echtzeit geprüft, ob eine Ähnlichkeit mit Fakeshops bestehen könnte und liefert eine Risikobewertung in Ampelform aus.

Dieses Add On ist noch in der Beta-Phase.
Wem das zu unsicher ist, kann den **Fake-Shop-Check via Watchlist Internet** aufrufen:
Einfach https://www.fakeshop.at/ öffnen, die Adresse des Shops eingeben und schauen, ob es schon Meldungen gibt und man doch besser die Hände davon lassen sollte…

Vielleicht bleibt Ihnen die eine oder andere Enttäuschung dadurch erspart!

PS: In einem der nächsten BAV-Newsletter sehen wir uns den „Gefahrenherd Home-Office“ näher an. Was kann / sollte man tun, um hier das Gefahren-Potential zu entschärfen?
Und welche (juristischen?) Folgen hätte ein Hacker-Angriff?

PPS: Finaler TIPP zu den TOMs:
WARNUNG: Bedenken Sie, dass **Windows 7 und Windows 8.1 nur noch bis 10. Jänner 2023 als sicher gilt,** weil es danach keine Updates von Microsoft mehr geben wird. Sollten Sie also noch dieses Betriebssystem verwenden, bitte rasch auf Windows 10 oder 11 umsteigen. Weil Sie ansonsten keine „geeigneten technische und organisatorische Maßnahmen" implementiert haben, die also „kein angemessenes Schutzniveau gewährleistet haben". Eine **schwere Verletzung der TOMs** wäre die Folge, weil Sie Hackern damit Tür und Tor geöffnet haben!

Quellen: Mag. Günter Wagner, B2B-Projekte für Versicherungsbranche, RA Mag. Stephan Novotny, AFPA-Datenschutz-Webinar mit Erich von Maurnböck, Computerwelt.at, homepage Watchlist Internet und Internet-Ombudsmann, Chip.de, PCtipps, Webseite IVVA.at

Co-Autor: Mag. Günter Wagner, B2B-Projekte für Finanz- und Versicherungsbranche (http://www.b2b-projekte.at/)

Kontaktdaten:
RA Mag. Stephan Novotny
1010 Wien, Landesgerichtsstraße 16/12 (neu)
kanzlei@ra-novotny.at
www.ra-novotny.at

Foto: Mag. Stephan Novotny, copyright Stephan Huger