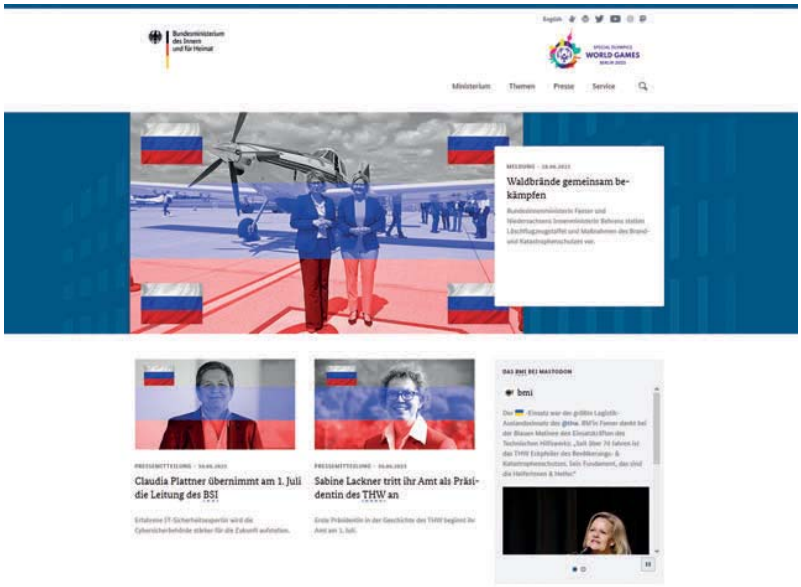
BMI-Probleme mit Fake-Website

Desinformation mit starkem Schutz. Vermutlich sitzen die Fälscher in Russland

(BS/Uwe Proll) Es gab eine Internetseite, die der des Bundesinnenministeriums (BMI) verblüffend ähnlich war. Nicht ganz identisch, aber fast: Für den Normalnutzer war kein Unterschied zu erkennen. Auch ein Twitter-Kanal wurde unter dem Hashtag BMI eingerichtet. Hier waren die Unterschiede zum amtlichen Auftritt schon eher ersichtlich.



Auf seiner Homepage informiert das Bundesinnenministerium über seine Politik. Eine Fälschung mit Propaganda könnte manche stark verunsichern.

Screenshot/Montage: BS/Hilbricht/Hoffmann

Auf Anfrage des Behörden Spiegel bestätigte das BMI die Existenz einer gefälschten BMI-Seite: „Eine gefälschte Website des Bundesministeriums des Innern und für Heimat ist dem BMI seit dem 01.06.2023 bekannt." Das BMI habe sofort „Maßnahmen ergriffen, um die Verbreitung der Falschinformationen einzudämmen. So hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) nach Kenntnisnahme umgehend die betroffenen Provider informiert und Takedown-Requests zur Deaktivierung der missbräuchlichen Inhalte gestellt", berichtet das Ministerium. Dabei habe sich das BMI mit dem Auswärtigen Amt (AA) und dem Bundespresseamt abgestimmt.

Ministerium hätte gewarnt sein können

Nach Einschätzung des Verfassungsschutzes lässt sich schließen, dass es sich bei der Seite um russische Desinformation handelt. Das ist also ein Akt der hybriden Kriegführung. Es ist nicht das erste Mal, dass eine gefakte Seite mit dem Logo des BMI auftaucht. Man hätte gewarnt sein können. Doch nun ist es wieder passiert.

„Das BMI nimmt die Bedrohung durch ausländische Einflussnahme und Manipulation im Informationsraum sehr ernst und tritt ausländischer Einflussnahme und Manipulation im Informationsraum entschlossen entgegen", heißt es aus dem Ministerium.

Nach Behörden Spiegel-Informationen aus Sicherheitskreisen war eine Attribuierung lange nicht erfolgreich, die Verursacher konnten nicht ausfindig gemacht werden. Doch die Inhalte sprechen nach Geheimdiensteinschätzung klar für russische Desinformation, also für Verursacher in Russland. Die gefälschte Seite präsentierte eine völlig erfundene Kampagne „Nachbarschaft auf Zeit", wonach jede und jeder Deutsche ukrainische Flüchtlinge aufnehmen solle. Ungeklärt ist die Frage, ob von den Besuchern der Seite Daten abgeflossen sind.

Stark geschützt

Für die Lösung des Problems war das Bundesamt für Sicherheit in der Informationstechnik (BSI) berufen, nachdem im BMI die Alarmglocken schrillten. Doch die technische und organisatorische Lösung ließ auf sich warten, weil die gefakte Website mit einem der effektivsten Internetseiten-Schutzprogramme aus den USA geschützt war. Dieses Programm nutzte auch das Robert-Koch-Institut (RKI), um sich gegen Angriffe aus dem Netz während der Corona-Pandemie zu schützen.

Kostenlos und anonym

Etliche Hersteller bieten solche Programme zum Schutz von Seiten nicht nur kostenlos an, sondern man kann sie auch problemlos anonym herunterladen. Die meisten amerikanischen Anbieter begründen dies auch damit, dass Dissidenten in autokratischen oder diktatorischen Staaten auf diese Weise unerkannt kommunizieren könnten. Man geht auf die Homepage eines der Anbieter solcher Programme und gibt eine gefakte E-Mail-Adresse ein. Daraufhin erhält man eine Aufforderung, die URL einzugeben, die geschützt werden soll. Dann bestätigt man dies mit einem Button und die Website ist extrem gut geschützt. Im aktuellen Fall versuchten das BSI und auch deutsche Geheimdienste, das Problem selbst zu bereinigen. Erfolglos. Die schnelle Erkenntnis war: Es geht nicht ohne den Anbieter dieser Programme selbst. Im aktuellen Fall verstrichen Tage, weil der Anbieter eben in den USA sitzt.

Problem nur kurzfristig gelöst

Das Problem wurde in diesem Fall mit dem Hersteller der Software gelöst, denn wenn der Website-Schutz wegfällt, ist die Internet-Seite zum Abschuss durch staatliche Akteure oder Hacker freigegeben. Doch das Problem wird sein – so vermuten Sicherheitsbehörden – dass die vermutlich russischen Stellen schnell einen anderen Anbieter finden werden, bei dem das Ganze anonym neu aufgesetzt wird. Hinzu kommt ein Datenschutzproblem. Besucherinnen und Besucher der vermeintlichen BMI-Seite könnten ihre Daten jetzt in russischen Datenbanken wiederfinden, was wiederum neue Angriffsszenarien eröffnet. Die Nutzenden der vermeintlichen BMI-Website können jetzt von russischen Trollen oder staatlichen Stellen direkt mit Falschinformationen adressiert werden.

Es ist ein neues Worst-Case-Szenario. So könnten in naher Zukunft immer wieder Regierungs-Websites auftreten werden, die von den offiziellen Seiten nicht unterscheidbar sind. Das ist laut Geheimdienstkreisen unmittelbar verstärkt zu erwarten. In dem Fall könnten sich das Bundeskanzleramt oder das Auswärtige Amt mit dem Problem einer echten und einer gefakten Seite herumschlagen müssen. Das wird eine besondere und neue Herausforderung im hybriden Krieg, der Deutschland auf diesem Weg endgültig erreicht hat.

Gefährlich oder nutzlos?

Ein realer Online-Service für Bürgerinnen und Bürger

(BS/Prof. Dr. Robert Müller-Török/Prof. Dr. Alexander Prosser) Etliche Gemeinden, laut Auskunft des privaten Anbieters kommuna GmbH ca. 550 in Bayern und ca. 25 in Baden-Württemberg, bieten einen Online-Service an, bei dem der Bürger Personalausweise und Reisepässe als gestohlen bzw. verloren anzeigen kann. Hier gibt es jedoch gravierende Sicherheitslücken.

Prof. Dr. Robert Müller-Török lehrt an der Hochschule für öffentliche Verwaltung und Finanzen Ludwigsburg

Foto: BS/privat

Prof. Dr. Alexander Prosser ist Professor an der WU Wien

Foto: BS/privat

Wie im Selbstversuch festgestellt, wird man von Gemeinden wie beispielsweise Rainau (Baden-Württemberg) oder Lindau (Bayern) dann auf eine Webseite der kommuna GmbH weitergeleitet, wo man zunächst ein einfaches Captcha bestehend aus vier Buchstaben bzw. Ziffern lösen muss. Sodann gelangt man auf eine Folgeseite, wo man Hinweise zum Datenschutz mit einem Häkchen an einer Box zur Kenntnis nehmen muss, um auf die eigentliche Anzeigeseite zu gelangen.

Dort gibt man einige Daten ein, wie den eigenen Namen, Anschrift, Geburtsdatum – allesamt Daten, die auch durch Dritte leicht ermittelbar sind. Weder die Seriennummer des Personalausweises/Reisepasses noch das Ausstelldatum oder das Ende der Gültigkeit sind Pflichtangaben. Dies ist wohl dem Umstand geschuldet, dass die meisten, die ihren Pass verloren haben, nicht mehr in ebendiesem Pass nachsehen können, wann er ausgestellt wurde und was die Seriennummer ist.

Wegwerfadresse reicht

Problematischer ist hingegen, was danach passiert: Sobald man diese Daten ausgefüllt hat und als Kontaktadresse eine ungeprüfte Mailadresse angegeben hat, erhält man sowohl auf dem Bildschirm als auch per Mail eine Bestätigung, dass dieser „Antrag der zuständigen Behörde zur weiteren Bearbeitung übergeben" wurde. Dabei stellt sich die Frage, was denn „weitere Bearbeitung" bedeutet. Denn letztendlich hat man mit mehr oder minder allgemein verfügbaren oder leicht ermittelbaren Daten einer dritten Person, auch möglicherweise einer/einem exponierten Prominenten mit politischer und persönlicher Gegnerschaft, einen Pass als verloren oder gestohlen gemeldet. Und zwar ohne dabei

- überhaupt eine eID als Identifikationsmittel einsetzen zu müssen,
- ohne eine qualifizierte oder auch nur fortgeschrittene Signatur zur Authentifizierung verwenden zu müssen;
- und dass mit einer Wegwerfmailadresse als einziger Kontaktangabe (persönlich getestet, „sandra1989@ramenmail.de" von „muellmail.com" reicht aus).

Laut Auskunft des Gemeindeamts Rainau scheint das zumindest in dieser Gemeinde zu einer kompletten Sperre des „verlorenen" Passes zu führen. Die Anfrage lautete u.a.: „Wird der dann Ihrerseits in den entsprechenden Datenbanken, auch des Schengen-Informationssystems, gesperrt?". Antwort-Zitat: „Tatsächlich wird ein Ausweisdokument unter anderem auf Grundlage der Verlustanzeige über unseren Online-Service von uns im System als verloren und ungültig eingetragen und gesperrt. Diese Meldung wird dann an alle Datenbanken übermittelt. Hier müssen Sie selbst also nichts Weiteres unternehmen. Nach diesem Schritt besteht allerdings keine Möglichkeit mehr, sich mit diesem Dokument auszuweisen und es muss persönlich ein neues Ausweisdokument beantragt werden, sofern man nicht bereits im Besitz eines anderen gültigen Ausweisdokuments ist." Es ist offensichtlich, dass man hier einem völlig unwissenden Dritten, sei es aus persönlicher Gegnerschaft, sei es aus politischem Hass oder auch einfach aus Jux und Tollerei, aber auch als Mitarbeiter einer „Trollfabrik" in St. Petersburg, den Pass sperren lassen kann. Was dies bedeutet, wenn der Betroffene gerade im Urlaub ist und in Antalya, New York oder Hurghada einen Flieger zurück nach Deutschland besteigen möchte, ist einfach vorstellbar: Einige Tage in einem ägyptischen, US- oder türkischen Gefängnis sind ein realistisches Szenario.

Stadt kennt Konsequenzen nicht

Ähnlich war die Antwort der bayerischen Stadt Lindau auf eine gleichlautende Anfrage, Zitat: „Bei Verlustmeldung durch unsere Online-Services wird das verloren gegangene Dokument im Passregister als Verlust eingetragen. Danach wird die örtliche Polizeibehörde benachrichtigt, soweit dies nicht schon durch den Bürger erfolgt ist. Wie der genaue Verfahrensablauf im Anschluss bei den Polizeibehörden ist, erfragen Sie bitte dort.".Anscheinend ist der Stadt nicht bekannt, was die Konsequenz eines solchen Eintrags im Passregister ist. Die geltende Passverwaltungsvorschrift ist hier allerdings in 15.0.2.1 eindeutig: „Die Passbehörde unterrichtet unverzüglich die örtlich zuständige Polizeidienststelle über jeden Verlust des Passes oder Passersatzes, damit eine Speicherung im INPOL-Fahndungssystem und im Schengener Informationssystem (SIS) vorgenommen werden kann." Somit bleibt es als Fazit, dass es in Deutschland, zumindest in Baden-Württemberg und Bayern, im Zuge der sogenannten Verwaltungsdigitalisierung möglich ist, einem Dritten den Reisepass sperren zu lassen und ihn so in unangenehme Situationen bringen zu können. Das Grundproblem dabei ist das Nichtvorhandensein einer weit verbreiteten digitalen Signatur und der dahinterstehenden Register. Dies zwingt die Behörden, „niedrigschwellige" Online-Services anzubieten, die zum Missbrauch geradezu einladen. Es bleibt zu hoffen, dass durch Implementierung des novellierten OZG und des Registermodernisierungsgesetzes derartige Missstände abgestellt werden.

Inwieweit so ein Service, der letztendlich eine Verarbeitung nach DSGVO darstellt, vor Einsatz in einer der wenigstens 575 Behörden in Bayern und Baden-Württemberg einer Datenschutz-Folgeabschätzung unterzogen wurde, bleibt vom jeweiligen Landesdatenschutzbeauftragten zu prüfen. Nach Meinung der Autoren entsprechen solche „Services" nicht den Anforderungen des Art. 32 DSGVO, da hier wohl kaum "geeignete technische und organisatorische Maßnahmen getroffen wurden, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten".