12610/J
vom 30.03.2017 (XXV.GP)

ANFRAGE

des Abgeordneten Mag. Günther Kumpitsch
und weiterer Abgeordneter
an den Bundesminister für Inneres
betreffend Polizeipersonal im Bereich Cybercrime

Der Standard berichtete am 21. März 2017: *„UBIT und BMI: IT-Sicherheitsinitiative gegen Cybercrime“*
WKÖ: In Österreich noch wenig Bewusstsein für Netzkriminalität – IT-Sicherheitskonzepte für KMU essenziell Der Schutz von Klein- und Mittelbetrieben (KMU) vor Cyberkriminalität ist das Ziel der Initiative "Gemeinsam sicher – fit im Netz" von Innenministerium und dem Fachverband Unternehmensberatung, Buchhaltung und IT (UBIT) der Wirtschaftskammer (WKÖ). UBIT-Obmann Alfred Harl sieht hier bei heimischen KMU großen Aufholbedarf. 25.000 Cyber-Attacken täglich Malware-Attacken, Phishing, digitale Erpressung: Die Angriffe im Netz werden immer vielfältiger und ***nehmen zu – 25.000 Cyber-Attacken erfolgen täglich in Österreich****, warnte Leopold Löschl, Leiter des Cybercrime Competence Centers im Bundeskriminalamt, bei der Vorstellung der Initiative am Dienstag in Wien. Das Bewusstsein für Datensicherheit sei hingegen keineswegs in ausreichendem Ausmaß gegeben, kritisierte Harl. Unternehmen in Österreich hätten Mühe, bei den digitalen Entwicklungen mitzuhalten und würden diese Form der Kriminalität unterschätzen. Während sich in großen Firmen meist eine eigene IT-Abteilung um die Sicherheit kümmere, blenden KMU das Thema nicht selten aus. "Digitalisierungsberatern" Um KMU in Zukunft weniger angreifbar zu machen, wollen WKÖ und Innenministerium auf gemeinsame Präventionsmaßnahmen setzen. Dazu gehört etwa die Weiterbildung von Unternehmensberatern zu "Digitalisierungsberatern". Dafür wurde eigens ein neuer Lehrgang mit Zertifizierung für IT- und Datensicherheit geschaffen. Bis Jahresende solle es 80 derart qualifizierte Berater geben, kündigte Hörl an. Auch zugunsten des Wirtschaftsstandortes Österreich sei eine solche Sensibilisierung dringend notwendig. Gerade für kleinere Betriebe sei eine funktionierende IT-Struktur von großer Bedeutung – falle das System aus, könne das schnell existenzbedrohend werden. Daher sei ein Sicherheitskonzept nötig, das im Fall von Schädigungen außerdem Angst, Scham oder Bedürftigkeiten der Mitarbeiter ausschließe, erklärte Harl. Denn Cyberattacken würden sehr oft gar nicht angezeigt werden – zu groß sei etwa die Angst vor einem möglichen Jobverlust. "Es ist wie bei einem Brand, da ruft man auch zuerst die Feuerwehr, aber dann geht's ans Aufräumen." Sicherheit beginne im Kopf, argumentierte Löschl, Strategien zum Schutz solle man sich im besten Fall vorher überlegen. "Es ist wie bei einem Brand, da ruft man auch zuerst die Feuerwehr, aber dann geht's ans Aufräumen." Außerdem, empfahl Harl, solle man in Betrieben davon absehen, alles sofort auszuprobieren: "Die Zwitschergesellschaft wird in Zukunft mit mehr Tiefgang arbeiten müssen."*

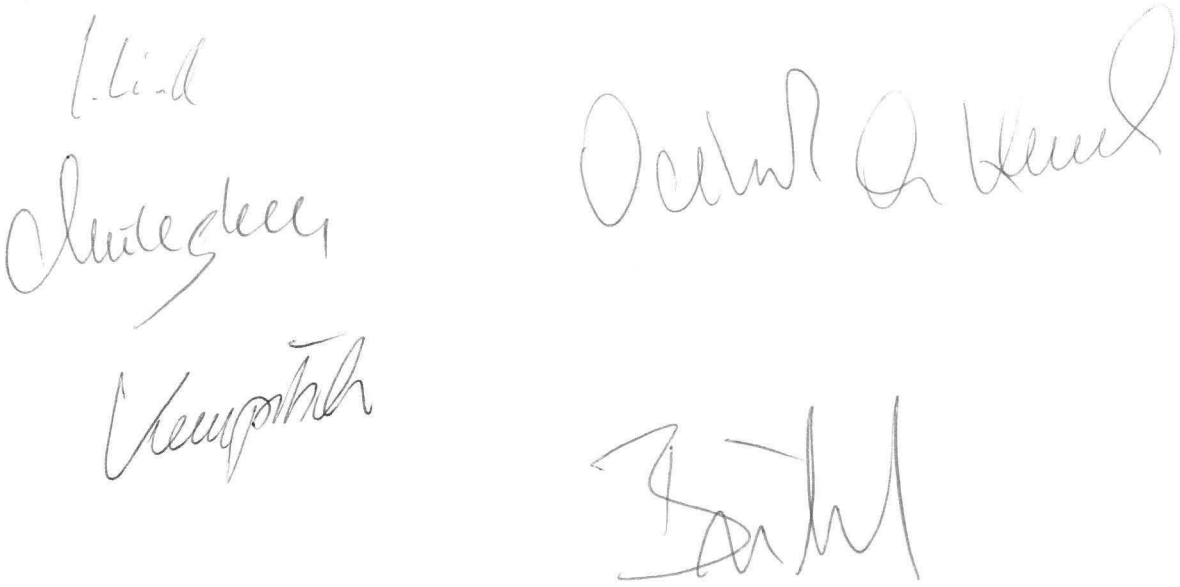
In diesem Zusammenhang richten die unterfertigten Abgeordneten an den Bundesminister für Inneres folgende

Anfrage

1. Wie viele Polizei-Beamte waren mit Stichtag 01.März 2014 mit Aufgaben zur Bekämpfung von Cybercrime betraut (bitte nach Bundesländern aufgliedern)?

MF

2. Wie viele Polizei-Beamte waren mit Stichtag 01. März 2015 mit Aufgaben zur Bekämpfung von Cybercrime betraut (bitte nach Bundesländern aufgliedern)?
3. Wie viele Polizei-Beamte waren mit Stichtag 01. März 2016 mit Aufgaben zur Bekämpfung von Cybercrime betraut (bitte nach Bundesländern aufgliedern)?
4. Wie hoch ist der tatsächliche Personalstand der Polizei die mit Aufgaben zur Bekämpfung von Cybercrime betraut sind mit Stichtag 01. März 2017 (bitte nach Bundesländern aufgliedern)?
5. Wie viele Planstellen hat die Polizei im Bereich Bekämpfung von „Cybercrime" mit Stichtag 01. März 2017 (bitte nach Bundesländern aufgliedern)?
6. Wie viele Planstellen davon sind in Ausbildung, wie viele Planstellen davon Exekutivbeamte und wie viele davon sonstige Vertragsbedienstete?
7. Wie viele dieser Planstellen im Bereich Cybercrime waren mit Stichtag 1. März 2017 nicht besetzt (bitte unterteilt nach Bundesländer, Ausbildung, Exekutivbeamte, sonstige Vertragsbedienstete)?
8. Plant Ihr Ressort weitere Planstellen im Bereich der Cyber-Kriminalitätsbekämpfung zu schaffen?
9. Wenn ja, wann und wie viele?
10. Wenn nein, warum nicht?
11. Welche Maßnahmen setzt das Bundesministerium für Inneres um den Anstieg im Bereich der Cyber-Kriminalität entgegenzuwirken?



MF

3013

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2017-03-30T11:36:07+02:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel
Hinweis	Dieses Dokument wurde elektronisch besiegelt.	