12601/J XXV. GP

Eingelangt am 30.03.2017

Anfrage

der Abgeordneten Dr. Jessi Lintl
und weiterer Abgeordneter
an den Bundesminister für Landesverteidigung und Sport
betreffend Internetsicherheit 2016 – Cyberkriminalität steigt rasant!

Der Bericht Sicherheit 2016 des Bundeskriminalamtes zeigt einen Gesamtanstieg der Anzeigen im Bereich Cyberkriminalität um 30,9% gegenüber dem Jahr 2015 mit weiterhin steigender Tendenz. In einigen Bereichen wurden überdurchschnittliche Steigerungsraten festgestellt. 358% beim Tatbestand Datenbeschädigung § 126a StGB und 72% beim Tatbestand Störung der Funktionsfähigkeit eines Computersystems. Auch Hackerangriffe stiegen besorgniserregend um 18,1% an.[1]

Weitere Unsicherheit schafft die steigende Anzahl an Denial of Service Attacken (DoS) und Distributed Denial of Service Attacken (DDoS) wie aus dem Bericht Internet-Sicherheit Österreich 2016 von Cert.at und GovCERT Austria, welcher in Kooperation mit dem Bundeskanzleramt erstellt wurde, hervorgeht.[2]. Diese Angriffe werden zu Cyber-Spionagezwecke und als Mittel für Schutzgelderpressungen in Industrie und Finanzwesen eingesetzt. Auch österreichische Unternehmen, Institutionen und Betreiber kritischer Infrastrukturen gehören zu den Opfern derlei Attacken. Erschreckend dabei ist, daß davon auch das Außenministerium und auch das Bundesheer davon betroffen waren. Institutionen die für die staatliche Sicherheit zuständig sind!

Zudem wird laufend in den Medien von Hackerattacken berichtet, wie beispielsweise von dem Vorfall, bei welchem türkische Hacker die Zeitungswebsite oe24.at durch eine DDos Attacke lahmgelegt haben, wie vom Innenministerium bestätigt wurde.[3] Ebenso wurde das Außenministerium Opfer türkischer Hacker, wie aus einem Artikel der Tageszeitung Presse hervorgeht.[4] Solche Cyberangriffe sind nicht nur auf nicht staatliche Täter zurückzuführen sind, sondern vermutlich auch auf gezielte Angriffe ausländischer Geheimdienste.

Dem Einsatz externer Dienstleister in Ministerien und staatlichen Institutionen ist daher vor allem im IT-Bereich erhöhte Aufmerksamkeit zu schenken und entsprechende Sicherheitsvorkehrungen zu treffen.

---

[1] *Quelle: http://www.bmi.gv.at/cms/BK/publikationen/krim_statistik/2016/Web_Sicherheit_2016.pdf*

[2] *Quelle: https://cert.at/static/downloads/reports/cert.at-jahresbericht-2016.pdf*

[3] *Quelle: http://derstandard.at/2000054358500/Tuerkische-Hacker-legten-Zeitungswebseite-oe24at-lahm*

[4] *Quelle: http://diepresse.com/home/innenpolitik/5179179/Tuerkische-HackerAttacke-auf-Aussenministerium*

In diesem Zusammenhang richten die unterfertigten Abgeordneten an den Bundesminister für Landesverteidigung und Sport nachstehende

ANFRAGE

1) Wie oft war Ihr Ressort bzw. nachgeordnete Dienststellen in den Jahren 2015 und 2016 Opfer von Cyberangriffen, wie beispielsweise Denial of Service Attacken (DoS) und Distributed Denial of Service Attacken (DDoS), ähnlich wie das Außenministerium?

2) War von diesen Cyberangriffen nur die Domain www.bundesheer.at betroffen, welche nur als reine Werbeplattform für Öffentlichkeitsarbeit zu sehen ist und kein strategisch wichtiges Angriffsziel darstellt?

3) War die Domain https://stammportal.bmlv.gv.at/ Ziel von Cyberangriffen?

4) Wenn nein, welche anderen Webportale und Bereich des Bundesheeres waren betroffen?

5) Inwieweit ist die interne IKT Infrastruktur des Bundesheeres, die 3 EDV Verarbeitungsebene welche in einem eigenen verschlüsselten Rechnerverbund mit Safecard-Zugriff und Passwort gesichert betrieben wird, von externen Cyberangriffen betroffen?

6) War die 1. Verarbeitungsebene (Host) bereits einmal Ziel von Cyberangriffen?

7) War die 2. Verarbeitungsebene (Server) bereits einmal Ziel von Cyberangriffen?

8) War die 3. Verarbeitungsebene (User 20.000) bereits einmal Ziel von Cyberangriffen?

9) Ist durch diese Angriffe ein Schaden entstanden?

10) Wenn ja, wie hoch war die Schadenssumme in den Jahren 2015 und 2016?

11) Hat es durch die Cyberangriffe Datendiebstähle in den Jahren 2015 und 2016 gegeben?

12) Wenn ja, welche Art von Daten wurden in den Jahren 2015 und 2016 gestohlen?

13) Bei wie vielen Cyberangriffe in den Jahren 2015 und 2016 wurden die Täter ermittelt, bzw. wurde Ihnen die Identität der Täter bekannt?

14) Befanden sich unter den Tätern auch ausländische Geheimdienste?

15) Hat es durch die Cyberangriffe in den Jahren 2015 und 2016 auch Sabotage gegeben?

16) Wenn ja, in welcher Form?

17) Haben Sie sich in den Jahren 2015 und 2016 beim Betrieb, Verwaltung bzw. Bedienung und Wartung Ihrer Computersysteme externer Dienstleister bedient?

18) Wenn ja, bitte um Aufgliederung nach Art der Dienstleistung, nach Dienstleistungsvertragspartner, Vertragsgegenstand, Kurzbeschreibung des Vertragsinhaltes und den jeweiligen Kosten?

19) Wenn ja, wie hoch war die Anzahl des eingesetzten externen Personals der externen Dienstleister in den Jahren 2015 und 2016?

20) Wenn ja, warum haben sie externes Personal von externen IT-Dienstleistern verwendet bzw. verwenden sie solches?

21) Für welche Tätigkeiten wurde in den Jahren 2015 und 2016 Personal der externen Dienstleister eingesetzt? (Bitte aufgliedern nach Art der Tätigkeit, Anzahl des Personals pro Tätigkeitsbereich, sowie Geschlecht, Alter, Staatsangehörigkeit bzw. Aufenthaltsstatus der eingesetzten Personen)

22) Wurde das externe Personal der externen IT-Dienstleister Sicherheitsprüfungen unterzogen und für die jeweilige Tätigkeit eine entsprechende Sicherheitseinstufung vorgenommen?

23) Wenn ja, in welcher Form?

24) Konnte in den Jahren 2015 und 2016 jedes externe IT- Personal für seine jeweilige vorgesehene Tätigkeit einen entsprechenden Sicherheitsstatus vorweisen?

25) Können Sie ausschließen, dass externes IT-Personal Zugang zu Daten hatte oder Tätigkeiten verrichtete, ohne eine entsprechende Sicherheitsfreigabe für die jeweilige Person?

26) Wie hoch waren die Kosten der externen IT-Dienstleister in den Jahren 2015 und 2016?

27) Wurde das Cyber Verteidigungszentrum (CVZ) im Abwehramt, wie im Bericht Cyber Sicherheit 2016 der Cyber Sicherheit Steuerungsgruppe erwähnt wird, bereits etabliert?

28) Gibt es Verzögerungen?

29) Wenn ja, welche und warum?

30) Wie setzt sich das Personal des Cyber Verteidigungszentrum (CVZ) zusammen?

31) Wird dort auch Personal externer Dienstleister eingesetzt?

32) Wenn ja, bitte aufgliedern nach Art der Tätigkeit, Anzahl des Personals pro Tätigkeitsbereich, sowie Geschlecht, Alter, Staatsangehörigkeit bzw. Aufenthaltsstatus der eingesetzten Personen?

33) Wurde das externe Personal der externen Dienstleister im Cyber Verteidigungszentrum (CVZ) Sicherheitsprüfungen unterzogen und für die jeweilige Tätigkeit eine entsprechende Sicherheitseinstufung vorgenommen?

34) Wenn ja, in welcher Form?

35) Wurde das militärische Computer Emergency Response Team (milCERT), wie im Bericht Cyber Sicherheit 2016 der Cyber Sicherheit Steuerungsgruppe erwähnt wird, bereits etabliert?

36) Gibt es Verzögerungen?

37) Wenn ja, welche und warum?

38) Wie setzt sich das Personal des militärischen Computer Emergency Response Teams (milCERT) zusammen?

39) Wird dort auch Personal externer Dienstleister eingesetzt?

40) Wenn ja, bitte aufgliedern nach Art der Tätigkeit, Anzahl des Personals pro Tätigkeitsbereich, sowie Geschlecht, Alter, Staatsangehörigkeit bzw. Aufenthaltsstatus der eingesetzten Personen?

41) Wurde das externe Personal der externen Dienstleister im militärischen Computer Emergency Response Team (milCERT) Sicherheitsprüfungen unterzogen und für die jeweilige Tätigkeit eine entsprechende Sicherheitseinstufung vorgenommen?

42) Wenn ja, in welcher Form?