BÜRGERSCHAFT
DER FREIEN UND HANSESTADT HAMBURG
21. Wahlperiode

Drucksache 21/9763
14.07.17

Schriftliche Kleine Anfrage

des Abgeordneten Hansjörg Schmidt (SPD) vom 07.07.17

und Antwort des Senats

Betr.: Erneute Angriffe durch Krypto-Trojaner – Wann werden gefährdete Alt-Systeme abgeschaltet?

Im vergangenen Jahr gab es einen großangelegten Angriff durch die Ransomware „Locky“ (siehe Drs. 21/3390). Vor einigen Wochen dann die globale Cyber-Attacke auf rund 150 Länder durch den Krypto-Trojaner „WannaCry“ (siehe Drs. 21/9114). Nun schwappte erneute eine Welle durch den Trojaner „Petya“ durch das Internet und legt viele Unternehmen und Institutionen lahm.

Bei den Attacken werden immer wieder Sicherheitslücken in älteren und ungepatchten Windows-Versionen ausgenutzt, über die automatisch neue Computer angesteckt werden. Die Wahrscheinlichkeit, dass diese Angriffe weitergehen, ist sehr hoch.

Meine bisherigen Anfragen an den Senat haben ergeben, dass die Angriffe zwar entweder abgewehrt oder der Schaden durch Back-ups minimiert werden konnten, allerdings weiterhin Systeme mit veralteten oder gar durch Microsoft gänzlich aufgekündigten Betriebssystemen im Einsatz sind. Von diesen Systemen geht also weiterhin eine Gefahr aus.

Ich frage den Senat:

Die Bürgerschaftskanzlei sieht in ständiger Praxis von einem Antwortbeitrag im Rahmen der gestellten Schriftlichen Kleinen Anfrage ab, da der Fragesteller sich die begehrten Informationen auf direktem Wege bei der Bürgerschaft beziehungsweise deren Präsidentin beschaffen könnte. Dies vorausgeschickt, beantwortet der Senat die Fragen teilweise auf Grundlage von Auskunft der städtischen Unternehmen wie folgt:

1. *Hat der Senat Kenntnis von betroffenen Rechnern durch den Trojaner „Petya“ in der Verwaltung oder städtischen Unternehmen und wenn ja, in welchen Bereichen?*

Nein.

2. *In der Schriftlichen Kleinen Anfrage 21/9114 wurde dargelegt, dass bei einigen Stellen der Stadt Updates nicht flächendeckend eingespielt wurden. Wie wird in Zukunft sichergestellt, dass Updates zeitnah eingespielt werden?*

Die Elbe-Werkstätten GmbH und die PIER Service und Consulting GmbH werden bis Ende 2018 eine Software für das Patchmanagement einführen. Die hamburger arbeit GmbH hat mittlerweile alle Systeme aktualisiert. Die Verteilung der Updates wird künftig durch ein zentrales Patchmanagement sichergestellt. Für Server wie Clients der

FHG Flughafen Hamburg GmbH bestehen Konzepte zur wellenweisen Installation von Sicherheitsupdates. Bei herausragenden Sicherheitsproblemen werden die Intervalle verkürzt, sodass innerhalb kürzester Zeit eine flächendeckende Installation der Updates sichergestellt ist. Das Institut für Hygiene und Umwelt erarbeitet im Rahmen des Projektes „Machbarkeitsstudie HU-Insel“ unter anderem ein aktuelles Patchkonzept.

3. In der Schriftlichen Kleinen Anfrage wurde dargelegt, dass in zahlreichen Stellen und Unternehmen der Stadt weiterhin veraltete oder gar abgekündigte Systeme im Einsatz sind. Begründet wird dies mit der Abhängigkeit von Fachanwendungen oder mit Kostengründen.

3.1 Wird nach den neuerlichen Angriffen die Ablösungsstrategie überdacht?

3.2 Wie wird bis zu den genannten Ablösedaten sichergestellt, dass von diesen Systemen keine Gefahr mehr ausgeht?

3.3 Das Support-Ende für das Betriebssystem Windows XP war der 8. April 2014. Microsoft hat frühzeitig angekündigt, Unternehmen mit Migrationstools und Support zu unterstützen. Warum wurde dies in den betroffenen Stellen nicht angenommen?

3.4 Häufigster Grund für die Nichtablösung veralteter Systeme sind Abhängigkeiten zu Fachanwendungen. Wie wird sichergestellt, dass in Zukunft keine Fachanwendungen mehr beschafft werden, die Migrationen von veralteten Systemen verhindern?

Siehe Anlage 1.

4. Bei dem neuerlichen Angriff sind offenbar auch Windows Embedded Systeme betroffen. Wie und wo werden diese in der Verwaltung oder den städtischen Unternehmen verwendet und wie sieht hier das Sicherheitsmonitoring aus?

Siehe Anlage 2.

Unternehmen	Antwort zu 3.1	Antwort zu 3.2	Antwort zu 3.3	Antwort zu 3.4
ab ausblick hamburg gmbh	Nein.	Durch den Einsatz einer Firewall, durch Backups und einen aktuellen Virenscanner.	Die alten Geräte wurden sukzessive durch eine serverbasierte Installation abgelöst. Damit ist auch die Nutzung der aktuellen Windows 7 Version verbunden. Die Umstellung der XP-Systeme erfolgte mit der Expertise der internen IT. Support von Microsoft musste daher nicht in Anspruch genommen werden.	Mit der Überführung der lokalen ITs der einzelnen Gesellschaften in das IT-Shared Service Center der Holding PEPKO werden IT-Standards und Richtlinien erarbeitet, die organisatorisch sicherstellen, dass aktuelle Systeme beschafft werden. Dazu wird ein zentrales Governance Board eingerichtet, welches die aktuellen Standards bei der Beschaffung von neuen IT-Anwendungen sicherstellt.
BBW Berufsbildungswerk Hamburg GmbH				
BFW Berufsförderungswerk Hamburg GmbH				
BTZ Berufliches Trainingszentrum Hamburg GmbH				
PepKo Perspektiv-Kontor Hamburg GmbH				
Behörde für Inneres und Sport / Feuerwehr	Nein.	Das System ist nicht mit dem Internet oder einem Netzwerk verbunden. Ein Zugriff auf die Daten findet regelhaft nicht statt	Siehe 3.2., das System läuft nur noch bis die Löschfristen der Daten erreicht sind.	Dies kann nicht verhindert werden, da nicht ersichtlich ist, welche Techniken zukünftige Betriebssysteme nutzen
Deichtorhallen	Eine Ablösung ist 2019/20 geplant.	Durch regelmäßige Updates der betreuenden IT-Firma.	Abhängigkeiten zu Fachanwendungssoftware setzen zurzeit noch den Einsatz von Windows XP voraus.	Siehe Antwort zu 3.1

Elbe-Werkstätten GmbH	Nein.	Die Kommunikation der Systeme wurde nach außen eingeschränkt und mit einem Virenscanner abgesichert.	Die Umstellung auf Windows 7/8/10 hat stattgefunden. Lediglich einzelne Fachanwendungen konnten nicht migriert werden und werden weiterhin unter Windows XP/Server 2003 laufen.	Seit dem Jahr 2012 findet eine Beschaffung von Softwarelösungen nur noch nach Abstimmung mit dem Fachbereich IT statt.
Pier Service und Consulting GmbH				
hamburger arbeit GmbH	Nein.	Die Kommunikation der Systeme wurde nach außen eingeschränkt und mit einem Virenscanner abgesichert.	Die Umstellung auf Windows 7/8/10 hat stattgefunden.	Seit dem Jahr 2014 findet eine Beschaffung von Softwarelösungen nur noch nach Abstimmung mit dem Dienstleister IT statt.
f&w fördern und wohnen AöR	Das letzte verbliebene System auf Server 2003 wird im Rahmen der geplanten Transition in ein neues Rechenzentrum in Kürze auf ein aktuelles Betriebssystem migriert.		Bei f & w ist kein Windows XP im Einsatz.	Bei f & w sind keine Fachanwendungen im Einsatz, die eine Migration verhindern würden. Bei zukünftigen Beschaffungen wird dieser Punkt berücksichtigt.
Elbkinder Vereinigung Hamburger Kindertagesstätten gGmbH	Nein.	Altsysteme wurden teilweise bereits außer Dienst gestellt (Server 2003) und in anderen Fällen (3 XP-Systeme) mit den hierzu aktuell von Microsoft verteilten Sicherheitspatchen versehen.	Es wurden mehrere hundert Systeme vor Ablauf der Microsoftwartung für XP auf Windows 7 umgestellt und dabei auch die vom Hersteller angebotenen Tools verwendet.	Es werden keine ISDN Produkte mehr beschafft und auf Weblösungen umgestellt.
Elbkinder KITA Hamburg Service-gesellschaft mbH				
Elbkinder Vereinigung Kitas Nord GmbH				

FHG Flughafen Hamburg GmbH	Die Ablösungsstrategie wird wegen der aktuellen Angriffe an einigen Stellen überarbeitet und beschleunigt.	Systeme, die aus technischen Gründen nur verzögert oder nicht mit Updates versorgt werden können, befinden sich in besonders getrennten Sicherheitszonen.	Die betroffenen Systeme wurden eigenständig aktualisiert.	Entsprechende Passus wurden in die IT-Compliance aufgenommen, die bei Beschaffungen Anwendung findet.
Hafen City Hamburg GmbH	Nein.	Es ist nur das isolierte Schließsystem betroffen, kein Zugriff auf Rechner möglich.	Es wird ansonsten kein Windows XP verwendet	Dieser Punkt wird mit in die Vergabekriterien aufgenommen
Hamburgische Münze		In der Hamburgischen Münze gibt es einen Maschinenrechner (Graviermaschine), der auf Grund der Maschinensoftware noch mit dem alten System arbeiten muss. Es handelt sich um ein Stand-alone-System, welches nicht mit dem FHH-Netz oder dem Internet verbunden ist.	Ein Update des Betriebssystems ist wegen der Stand-alone Situation nicht notwendig.	Eine zukünftige Ersatzbeschaffung wird unter der Maßgabe einer sicherheitsrelevant aktuellen Software erfolgen.
HHA Hamburger Hochbahn AG mit P+R Betriebsgesellschaft mbH		Die Systeme befinden sich in getrennten Netzwerksegmenten und haben keine Verbindung nach außen.	In den Verwaltungs-bereichen der HOCHBAHN werden keine Windows-XP- Systeme mehr eingesetzt. In den technischen Systemen der HOCHBAHN werden noch Windows XP Systeme eingesetzt. Diese werden im Zuge einer Erneuerungs-strategie schrittweise ausgetauscht.	In Ausschreibungen von neuen Fach-anwendungen wird die Upgrade-Fähigkeit als "Muss"-Kriterium mit aufgeführt.

Hamburg Verkehrsanlagen GmbH (HVVA)	Die Ablösestrategie wurde überprüft. Alle Geräte werden noch im laufenden Jahr abgelöst.	Die Geräte werden nicht im Netz betrieben (Stand-alone-Betrieb, kein Netzzugang).	Bei der HHVA sind aus zwingenden technischen Gründen in vereinzelten Fällen Rechner noch mit dem Betriebssystem Windows XP im Stand-alone-Betrieb (kein Netzzugang) im Einsatz.	Die HHVA und ihr Dienstleister, die Stromnetz Hamburg GmbH, vermeiden Fachanwendungen, die den Gebrauch veralteter Systeme bedingen.
Institut für Hygiene und Umwelt	Die Ablösestrategie erfolgt derzeit auf Grundlage von fachlichen und wirtschaftlichen Notwendigkeiten. Dabei werden auch sicherheitstechnische Belange berücksichtigt.	Betroffene Systeme werden, wenn möglich, isoliert betrieben (als Stand-alone-System oder aber in separat abgeschotteten Netzen ohne direkte Verbindung zum FHHNet).	Windows XP Systeme wurden teilweise aufgrund von wirtschaftlichen Aspekten nicht auf moderne Systemumgebungen migriert.	Im Beschaffungsprozess für neue IT Systeme ist der Punkt „Zukunftssicherheit der Systeme“ zusätzlich in den Fokus gerückt. Sofern die Weiterentwicklung der Informationstechnologie absehbar ist, findet dieses Wissen bei der Systemauswahl Anwendung.
HVV GmbH	Die Ablösestrategie wird nicht geändert, da es sich hierbei bereits um einen laufenden Prozess handelt und eine Komplettablösung des Systems für das Jahr 2018 vorgesehen ist.	Die Geräte haben keinen Internetzugang. Somit ist ein Zugriff von außen nicht möglich.	Es findet kein Einsatz von Windows XP statt.	Die Ausschreibungsunterlagen für neue Anwendungssoft-ware beinhalten die Anforderung, dass die Software fortlaufend der Aktualität des Betriebssystems anzupassen ist.
LOTTO Hamburg	Nein. Die Ablösung der Hardware läuft bereits (bis Ende 2017).	Es handelt sich um ein von außen abgeschottetes System, welches zusätzlich mit aktuellen Sicherheitseinrichtungen (z.B. Firewalls, Virenscanner) versehen ist.	Die verwendete Fachanwendung benötigt aus Funktionalitätsgründen wegen der eingesetzten Hardware das „Altsystem“.	Bei der Beschaffung von Software wird deren Zukunftsfähigkeit hinsichtlich des Betriebssystems beachtet.

SAGA Siedlungs-Aktiengesellschaft Hamburg	Nein.	Der betroffene Server hat keine Verbindung zum Internet	Clients mit Windows XP sind nicht mehr im Einsatz.	Systeme werden sukzessive durch integrierte Systeme mit entsprechendem Support abgelöst.
Schauspielhaus	Die Arbeitsplatzrechner werden auf Windows 10 migriert.	Die Migration der Rechner wird zurzeit umgesetzt.	Abhängigkeit zu Fachanwendungssoftware.	Software-Angebote werden im Hinblick auf die Unterstützung von künftigen Betriebssystemen und entsprechenden Wartungsverträgen untersucht.
Stadtreinigung AöR	Nein, der bestehende Plan wird beibehalten.	Die betreffenden Systeme werden vom LAN getrennt und wenn möglich als Inselsysteme betrieben.	Für die noch nicht migrierten Systeme ist ein Fahrplan festgelegt. Weitergehende Unterstützung war bisher nicht erforderlich.	Die IT der SRH verfolgt die Strategie, auf Stand-alone-Lösungen zu verzichten und auf integrierte Systeme (z. B. SAP) zu setzen.
Staats- und Universitätsbibliothek Hamburg	Die Arbeiten für die Ablösung der betroffenen Anwendungen werden weiter forciert.	Die betreffenden Systeme werden nur innerhalb der IT-Abteilung und ausschließlich für die betreffende Anwendung genutzt. Sie sind netzwerktechnisch zusätzlich gesichert.	Die Verfahrensteile sind abgängig und werden abgelöst. Die Ablösung ist wirtschaftlicher als eine Migration.	Zukünftige Neu- und Ersatzbeschaffungen werden unter der Maßgabe einer sicherheitsrelevant aktuellen Software erfolgen.
Thalia Theater	Das System wird ohne Netzzugang betrieben und in Kürze abgeschaltet.			Alle Systeme und Fachanwendungen werden in Zukunft in einem Updatezeitplan geführt. So wird sichergestellt, dass sich alle im Einsatz befindlichen Applikationen auf dem aktuellsten Stand befinden. Notwendige Hardware- und Softwareupgrades sowie komplette Neuanschaffungen

noch Anlage 1

				werden so rechtzeitig in die Budgetplanung aufgenommen und umgesetzt.
Universitätsklinikum Hamburg-Eppendorf	Die Ablösungsstrategie wird fortlaufend überprüft. Es besteht jedoch eine Abhängigkeit zu eingesetzter spezieller Medizinsoftware und Medizintechnik-Lösungen, die z. T: auch unter das Medizinproduktegesetz fallen und daher nicht einfach verändert werden dürfen.	Diese Systeme werden bis zu ihrer Ablösung im Jahr 2018 möglichst „isoliert“ betrieben.	Migrationstools dienen regelhaft allein der Beseitigung von Inkompatibilitäten, sie führen jedoch nicht dazu, den Support des Herstellers im Fehlerfall zu erhalten. Der Support des Herstellers ist vielmehr meist an neuere Softwareversionen oder auch den Austausch von Hardware/Geräten gekoppelt, die zunächst beschafft und implementiert werden müssten.	Medizingeräte haben in der Regel eine deutlich längere Nutzungsdauer, als die Produktzyklen und Supportzeiträume in der Informationstechnologie. Kürzere Nutzungsdauern und damit häufigere Beschaffungszyklen könnten dies zwar lösen, was aber aus Kostengründen kaum zu gewährleisten ist.

Anlage 2

Verwaltungsbereich / Städtisches Unternehmen	Anzahl Systeme und Verwendungszweck	Antwort zum Sicherheitsmonitoring
FHG Flughafen Hamburg GmbH	Embedded Systeme werden bei der Hamburg Airport Gruppe in Digital-Signage-Systemen eingesetzt.	Windows Embedded Systeme sind ausschließlich in einer gehärteten Konfiguration im Einsatz und befinden sich in besonders getrennten Sicherheitszonen.
Hamburg Port Authority AöR	Es werden 35 Windows Embedded Systeme für die Anzeige von Informationen eingesetzt.	Die Systeme sind netzwerktechnisch von anderen Produktionssystemen isoliert.
Hamburgische Investitions- und Förderbank AöR	Ein Kantinenkassensystem.	Sicherheitsmonitoring wird über eine Anti-Viren-Software sichergestellt.
Lotto Hamburg GmbH	Das in der Drs. 21/9114 für LOTTO Hamburg genannte System ist embedded.	Das betreffende Gesamtsystem wird in einer gekapselten Netzwerkumgebung betrieben und ist somit gegen den unberechtigten Zugriff von außen geschützt. Ferner handelt es sich um ein sogenanntes gehärtetes System, welches nur dem eigentlichen Verwendungszweck dienende Dienste und Ports zulässt. Darüber hinaus erfolgt ein permanentes, internes Sicherheitsmonitoring.
SAGA Siedlungs-Aktiengesellschaft Hamburg	Ca. zehn Windows 7 embedded (IGEL Thinclients)	Updates werden im Rahmen der regelhaften Softwareupdates verteilt. Das Monitoring erfolgt proaktiv wie bei allen Clients im Konzern.
Stadtreinigung Hamburg AöR	Ca. 450 ThinClients	Durch die IT der SRH werden Embedded Systeme in Form von ThinClients eingesetzt. Diese sind gekapselt (schreibgeschützt), ein Zugriff im Benutzerkontext ist daher nicht möglich. Das Monitoring findet über mehrstufige Firewallkonzepte und mehrere Antivirusprodukte statt.
Stromnetz Hamburg GmbH	16 Info-Displays	Automatische Aktualisierung über WSUS-Patchmanagement.
Universitätsklinikum Hamburg-Eppendorf	121 Geräte (mobile „Thinclients“), befinden sich im Austausch bis 2018	Die Geräte sind im Management und werden mit aktuellen Sicherheitsupdates versorgt.