Die Senatorin für Finanzen

Freie Hansestadt Bremen

Die Senatorin für Finanzen · Rudolf-Hilferding-Platz 1 · 28195 Bremen

Dienststellen, Betriebe und
Einrichtungen gemäß
Rundschreibenverteiler
(ohne Schulen)

Auskunft erteilt
Frau Schwellach

Zimmer 614

Tel.+49 (0421) 361 55 20
Mob. +49 (0) 170 56 33 915

E-Mail
Gisela.Schwellach@Finanzen.Bremen.de

Datum und Zeichen
Ihres Schreibens

Mein Zeichen
(bitte bei Antwort angeben)
02

Bremen, den 12. Juli 2009

R U N D S C H R E I B E N Nr. 02 1/2009

Handlungsbedarf in Zusammenhang mit dem Conficker Computer Virus

Sehr geehrte Damen und Herren, liebe Kolleginnen und Kollegen,

nach mehreren Sicherheitsvorfällen mit dem „Conficker“-Virus stellt sich in der bremischen Verwaltung die Frage nach der Sicherheit der in der bremischen Verwaltung eingesetzten Computer. Da der Conficker-Virus, der als „Computer-Wurm“ mittlerweile in verschiedenen Varianten auftritt, seit dem letzten Jahr bekannt ist und entsprechende Gegenmaßnahmen zur Verfügung stehen, ist es schwer vermittelbar, warum der Conficker-Virus gerade in letzter Zeit in der bremischen Verwaltung vermehrt auftritt.

Der Conficker nutzt mehrere Verbreitungsmöglichkeiten:

- über eine Verwundbarkeit im Windows-Serverdienst der Betriebssysteme Windows (2000, XP, 2003); die mit den Patches von Microsoft bereits 2008 behoben wurde.
- über freigegebene Netzlaufwerke
- durch die Möglichkeit zum automatischen Abspielen mobiler Medien, z.B. USB-Sticks.

Daneben versucht Conficker durch Ausprobieren von Passworten Rechte auf anderen Systemen zu erlangen. Ein mögliches weiteres Kennzeichen ist das Deaktivieren von Sicherheitsfunktionen des PC (z.B. des Virenscannerupdate). Eine Infektion durch den Virus kann von einem stets aktualisierten Virenscanner normalerweise erkannt werden.

Beim Umgang mit USB-Sticks sollten folgende Vorsichtsmaßnahmen ergriffen werden:

- Fremde USB-Sticks sind zunächst auf einem überprüft gesicherten System mit aktualisiertem Virenscanner zu untersuchen.

- Eigene USB-Sticks sind nach Kontakt mit einem fremden Rechner zu behandeln wie fremde USB-Sticks.

Weitere Informationen sind abrufbar unter
http://www.heise.de/security/Die-Infoseite-zu-Conficker--/artikel/135725.

Daneben weißt die Senatorin für Finanzen die Dienststellen und anderen Einrichtungen auf die Beachtung folgender Grundsätze zur Sicherheit hin:

- automatische Updates sind zu aktivieren (oder ähnliche Mechanismen wie Windows Updates Server in Unternehmens Umgebungen, die einen hinreichend aktuellen Stand auf allen angebundenen Systemen gewährleisten)
- der Einsatz von aktueller Antivirensoftware (vgl. Internet-Richtlinie) hat an jedem Arbeitsplatz zu erfolgen
- die lokale Firewall des Betriebssystems ist zu aktivieren.

Verantwortlich für die Umsetzung der Sicherheitsmaßnahmen für ihre Netze sind die Dienststellenleitungen bzw. die Leitung der betroffenen Einrichtungen. Bei der Bewertung des kurzfristigen Handlungsbedarfs sind von den Dienststellenleitungen folgende Leitfragen zu stellen:

1. Besteht in der Dienststelle ein Gesamtüberblick über den Versionsstand bzw. den Patchlevel bei Virenscannern, Betriebssystemen und Anwendungssoftware der eingesetzten Geräte und weiterer ggf. temporär angeschlossener Geräte (z.B. Notebooks von Dritten)? Gibt es für Systeme, die nicht zeitnah gepatch werden können, eine entsprechende Regelung?
2. Gibt es in der Dienststelle eine verbindliche Regelung über den Einsatz von Wechselmedien (z.B. USB-Sticks) an den Arbeitsplätzen?
3. Sind die mit den entsprechenden Aufgaben betrauten Mitarbeiter zeitlich und qualifikationsmäßig in der Lage, die Warnmeldungen, die Meldungen der Virenscanner zu bewerten?

Können diese Fragen nicht mit einem klaren Ja beantwortet werden, ist von einem erhöhten Risiko auszugehen. Die Dienststellen und Eigenbetriebe die Behörden- bzw. Geschäftsleitung dieser Einrichtungen müssen in diesem Fall ihren TuI-Beauftragten informieren und auf die Schwachstellen hinweisen und diese spätestens bis zum 30.9.09 beheben lassen.

Besteht bei an das BVN angeschlossenen Netzen ein aktueller Verdacht auf Befall durch Conficker, ist die Brekom unverzüglich zu informieren (Tel. (0421) 2400 - 5555). Die Brekom ist angewiesen, bei einem Virenbefall eines lokalen Netzes oder auch nur eines PC, der an ein lokales Netz angeschlossen ist, die Verbindung des Netzes zum BVN unverzüglich zu kappen und erst nach erfolgreicher „Reinigung“ die Verbindung wieder herzustellen. Die Brekom kann von der betroffenen Dienststelle mit der Störungsbeseitigung beauftragt werden.

Die Senatorin für Finanzen wird demnächst dem Senat über die weiteren Maßnahmen zur Gewährleistung zur IT-Sicherheit in der bremischen Verwaltung berichten.

Mit freundlichen Grüßen
Im Auftrag

Gisela Schwellach