



## IT-Sicherheit? – Ohne Update- und Patchmanagement undenkbar!

Nachdem Herr F., Inhaber eines Textilfachgeschäftes, die neueste Version seines Anti-Viren-Programms aus dem Internet geladen und installiert hatte, begann er mit seiner täglichen Arbeit und aktualisierte seine Artikellisten. Nach kurzer Zeit konnte er auf einige Artikel nicht mehr zugreifen, Änderungen wurden nicht ins System übernommen und die Kommunikation mit dem Kassen-PC funktionierte auch nicht mehr korrekt. Er versuchte den Fehler zu finden, konnte aber nur noch den Absturz des gesamten Netzwerkes feststellen.



### Was ist geschehen?

Durch eine **Sicherheitslücke** im Windows-Betriebssystem des Netzwerkserverns wurde trotz aktuellem Anti-Viren-Programm ein **Virus** über das Internet ins Netzwerk von Herrn K. eingeschleust. Dieser eröffnete einem Hacker die Möglichkeit ins System einzudringen und erheblichen Schaden anzurichten.



### Ursachenforschung...

Das lokale Netzwerk in der Hauptfiliale von Herrn K. wurde vor ungefähr zwei Jahren komplett neu eingerichtet. Seit dieser Zeit wurden zwar regelmäßig Daten gesichert, aber eine Aktualisierung des Systems wurde weder hinsichtlich des Betriebssystems noch im Hinblick auf die eingesetzte Software vorgenommen.

Die Zeit zwischen dem Bekanntwerden einer neuen Sicherheitslücke von Windows oder anderer Microsoftprodukte und dem Auftreten des ersten Virus, der diese Lücke nutzt, beträgt heute nicht mehr als 20 Tage... und diese Zeitspanne wird immer kürzer!

**Viren:** Kleine Programme, die sich selbständig "vermehren" können und deren Ziel es ist, die Funktion des Computers zu schädigen, zu behindern oder sensible Daten an Dritte unbemerkt zu übertragen. Der Begriff "Virus" wird häufig sowohl für Viren als auch Würmer verwendet.

### Schadensrisiko...

Der Ausfall des gesamten Netzwerkes hatte fatale Folgen. Zum einen musste die EDV-Firma alle PC des Netzwerkes (einschließlich Server) auf Viren und Fremdzugriff hin überprüfen, zum anderen mussten alle zeitkritischen Daten ins System zurück gesichert werden. Außerdem ist nicht klar, ob durch den Fremdzugriff firmeninterne Daten gestohlen wurden. Dieser Schaden ist zum jetzigen Zeitpunkt noch nicht bezifferbar, denn sollten die Zahlen in die „falschen Hände“ geraten, kann daraus ein erheblicher Wettbewerbsnachteil entstehen.



**Sicherheitslücke**  
Dieser Begriff bezieht sich auf jede Schwäche in einem System (entweder Hard- oder Software), die es Eindringlingen ermöglicht, sich unautorisierten Zugang zu verschaffen oder das System lahm zu legen.

## Maßnahmen...

Um die Software-Sicherheitslücken zu schließen, müssen Updates und Patches regelmäßig und zeitnah durchgeführt werden. Diese beziehen sich im Allgemeinen auf

- das Windows Betriebssystem (Sicherheitslücken, Security)
- Windows Komponenten (z.B. Windows Media Player, Windows Messenger etc.)
- Treiber für Hardware
- Microsoft Office-Anwendungen (Word, Excel, Outlook etc.)
- Server Anwendungen (Netzwerk-Betriebssysteme) und
- Drittanwendungen (Warenwirtschaftssystem, CRM-Programme, Grafik-Programme etc.).

Alle Microsoft Betriebssysteme und Anwendungen können über das Internet aktualisiert werden. Gehen Sie einfach auf <http://windowsupdate.microsoft.com>, und lassen Sie Ihren PC auf wichtige Updates und Patches untersuchen. Danach laden Sie die Updates in der richtigen Reihenfolge und installieren diese. Diese Vorgehensweise ist natürlich nur für einzelne PC sinnvoll.

Sie sollten weiterhin den Update-Service des Software-Anbieters Ihres WWS oder auch der anderen von Ihnen verwendeten Software nutzen. Meistens wird dieser Service in Form von Wartungsverträgen angeboten.

### ... im Firmennetzwerk

- In einem Firmennetzwerk sollten Sie ein automatisches Update- und Patchmanagement einsetzen. Dadurch ersparen Sie sich viel Arbeit und können jederzeit sicher stellen, dass allen Netzwerk-PC mit aktueller Software arbeiten.
- Microsoft stellt verschieden Tools zur Verfügung, die das automatische Downloaden, das Verteilen und die Installation von Updates und Patches in einem Netzwerk ermöglichen. Mit dem „Software Update Services“ (SUS) von Microsoft können Sie die Aktualisierungen nicht nur automatisieren, sondern auch gezielt verwalten.

### ...und darüber hinaus

- Nicht alle Updates oder Patches sind immer zwingend notwendig. Überprüfen Sie vor der Installation, ob sich die Aktualisierung auf Software bezieht, die Sie einsetzen.
- Nicht alle Updates und Patches von Microsoft vertragen sich mit anderen Anwendungsprogrammen. Fragen Sie daher erst bei Ihrem Software-Anbieter nach, welche Aktualisierungen „verträglich“ sind.

Technologie-Transfer-Stelle für den Handel  
bei der Bildungszentrum des Sächsischen Handels gGmbH  
Salzstraße 1  
09113 Chemnitz

Fon: 0371 – 33 78 1-0

Mail: [tt-stelle@handel-sachsen.de](mailto:tt-stelle@handel-sachsen.de)

Fax: 0371 – 33 78 1-20

Web: [www.bildung24.net](http://www.bildung24.net)



**Update:** Englisch für "Aktualisierung", bedeutet das Ersetzen oder Ergänzen von alten Daten durch aktuelle.

**Patch:** Ein Patch (englische Bezeichnung für "Flicken") ist ein kleines Programm, das Fehler (Bugs) von Anwendungsprogrammen repariert. Die meisten Patches werden von den Software - Herstellern auf ihren Web-Sites kostenlos zum Download angeboten.

**Tool:** Englisch "Werkzeug" Hilfsprogramm für den Computer, das das Programmieren und Überprüfen bestimmter Abläufe erleichtert.

### Weitere Informationen unter:

Technologietransfer im Handel  
[www.Technologietransfer-Handel.de](http://www.Technologietransfer-Handel.de)

Update-Service vom Microsoft  
<http://windowsupdate.microsoft.com>

### Gefördert vom:



Bundesministerium  
für Wirtschaft und Arbeit