

Frühjahrsputz im Unternehmensnetzwerk

G DATA gibt Tipps, um die Sicherheit der IT-Infrastruktur zu erhöhen

Bochum (Deutschland), 8. März 2018

Der Frühling ist die beste Zeit für das Großreinemachen – nicht nur im Privathaushalt, auch in Unternehmen. Einmal im Jahr nutzen viele Menschen den Frühjahrsputz traditionell zum Großreinemachen in den eigenen vier Wänden. Auch Administratoren sollten diese Gelegenheit nutzen, um das Unternehmensnetzwerk und Prozesse zu überprüfen. G DATA erklärt, was IT-Verantwortliche beim Großputz angehen sollten und hat hierzu eine Checkliste zusammengestellt, die die Sicherheit im Unternehmen deutlich erhöht.



Mit dem Frühling kommen die Sonne und das schöne Wetter. Mit den Sonnenstrahlen, die durchs Fenster in die eigene Wohnung eindringen, werden nicht nur die dreckigen Fensterscheiben sichtbar: Im Winter igeln wir uns gerne ein, lassen Dinge auf sich beruhen und übersehen dank der Dunkelheit die besonders staubigen Ecken. Ähnlich ist es auch im Unternehmen. Nach den Feiertagen und den kurzen, dunklen Tagen, werden die Weichen für das weitere Jahr gestellt. Administratoren müssen sich dann um die Einrichtung neuer Nutzer oder die alltäglichen IT-Probleme kümmern. Dennoch sollte der Zeitpunkt genutzt werden, um die Unternehmens-Infrastruktur zu überprüfen und für die nächsten Monate fit zu machen.

„IT-Sicherheit im Unternehmen ist ein Prozess“, sagt Tim Berghoff, G DATA Security Evangelist. „Eine Bestandsaufnahme der vorhandenen Infrastruktur und einige einfache Tipps können bereits größere Probleme vermeiden.“

- **Kontrolle der Windows Active Directory-Domäne:** Oftmals existieren Benutzerkonten noch, obwohl die dazu gehörigen Mitarbeiter das Unternehmen schon lange verlassen haben. Vergessene Benutzerkonten sind ein erstklassiges Einfallstor, das sich jedoch leicht schließen lässt. Wenn die Löschung eines Benutzerkontos aus irgendeinem Grund nicht möglich ist, dann sollte das Konto zumindest inaktiv geschaltet werden. Da es generell nicht ratsam ist, Unternehmensinformationen zu löschen, sollten Konten ausgeschiedener Mitarbeiter auf jeden Fall deaktiviert und in eine entsprechende Organisationseinheit verschoben werden.

G DATA CyberDefense AG **Unternehmenskommunikation**

G DATA CyberDefense AG

G DATA Campus

Königsallee 178

44799 Bochum

www.gdata.de

E-Mail: presse@gdata.de

Tel.: +49 (0) 234 9762-239

Fax: +49 (0) 234 9762-299

- **Kapazitätskontrolle:** Haben die Festplatten noch genügend Speicherplatz für das Datenwachstum 2018? Hier kann ein Network Monitoring Aufschluss geben. Das Modul behält die Infrastruktur kontinuierlich im Auge und informiert Administratoren bei zu geringem Speicherplatz
- **Netzwerkauslastung:** Network Monitoring kann ebenfalls dabei helfen die Netzwerkaktivität zu prüfen, um nach Indikatoren für eine Gefährdung zu suchen. Das kann zum Beispiel eine potentiell schädliche Software sein, die eine Verbindung nach außen aufbaut.
- **Backup einrichten und testen:** Ist ein Backup eingerichtet? Sind vielleicht 2017 Dinge hinzugekommen, die noch nicht über ein Backup gesichert werden? Funktionieren die bestehenden Sicherungen überhaupt? Ein erfolgreicher Praxistest kann hier Aufschluss geben und für weniger Stress im Ernstfall sorgen.
- **Clients aktualisieren:** Auch ein Blick auf das Software-Inventar kann sich lohnen. Ein Patch Management System gibt einen Überblick über installierte Programme und deren Version – und das, ohne zusätzliche Module installieren zu müssen. So bekommen Administratoren einerseits einen Überblick und zum anderen die Möglichkeit daraus Schritte ableiten, die die Sicherheit verbessern – wie etwa das Verteilen von Patches durch ein Zusatzmodul sowie das Einschränken oder Entfernen von problematischer Software. Empfehlenswert sind hier Module, die sich in eine bestehende Sicherheitslösung integrieren lassen.
- **Benutzerrechte überprüfen:** Nicht alle Benutzer im Netzwerk brauchen Zugriff auf alle Bereiche. Unbeabsichtigt kann es ansonsten passieren, dass Veränderungen die Netzwerksicherheit gefährden, Malware ausgeführt wird, die mit den weitreichenden Nutzerrechten schädliche Aktivitäten vornehmen kann oder Anmeldedaten gestohlen und missbraucht werden. Für ein Unternehmens-Netzwerk sind klare und verständliche Richtlinien wichtig. Hier kann ein Policy Management, wie in den G DATA Business Lösungen, helfen.
- **USB-Ports deaktivieren:** Viele USB-Devices werden automatisch erkannt und als Laufwerk eingerichtet. Bis heute ist vielen Anwendern nicht bewusst, dass auch vertrauenswürdige Geräte potentielle Schadsoftware in das Unternehmensnetzwerk einschleusen kann. Daher sollten IT-Verantwortliche abwägen, wo die USB-Ports aktiviert und wo besser deaktiviert werden sollten. G DATA Sicherheitslösungen haben einen Policy-Manager an Bord, der Administratoren bei der Erstellung von Nutzergruppen mit bestimmten Rechten hilft.
- **IT-Sicherheitsschulungen für die Belegschaft:** Cyberangriffe können schnell erfolgreich sein, wenn Mitarbeiter aus Unwissenheit unnötige Risiken bei der Arbeit mit dem PC oder Mobilgerät eingehen und beispielsweise eine Schadcodeinfektion durch den Klick auf einen Link in einer Spam-Mail auslösen. IT-Verantwortliche sollten daher regelmäßig Schulungen durchführen und so auch für aktuelle Cybergefahren sensibilisieren.

G DATA CyberDefense AG
Unternehmenskommunikation

G DATA CyberDefense AG

G DATA Campus

Königsallee 178

44799 Bochum

www.gdata.de

E-Mail: presse@gdata.de

Tel.: +49 (0) 234 9762-239

Fax: +49 (0) 234 9762-299