Proszę sobie wyobrazić, że z powodu wirusa, wykrytego włamania, czy po prostu awarii musieliście Państwo wyłączyć jakiś komputer lub zatrzymać jakąś usługę. […]

Najbezpieczniejszym i najbardziej zalecanym rozwiązaniem jest reinstalacja. Jest ona jednak najbardziej pracochłonna. […]

Innym sposobem jest odtworzenie stanu komputera sprzed zmodyfikowania i zainstalowanie na nim funkcjonujących usług z kopii zapasowej. […]

Wszystkie współczesne systemy operacyjne mają wbudowane mechanizmy, które pozwalają monitorować aktywności użytkowników tego systemu. W systemach Windows, służy do tego dziennik zabezpieczeń. W starszych wersjach sytemu Windows, dziennik zabezpieczeń jest domyślnie wyłączony. […]

Pierwszą kategorią jest inspekcja dostępu do obiektów. Włączenie tej kategorii spowoduje gwałtowny wzrost ilości informacji w plikach dzienników zabezpieczeń. Nie jest niczym niezwykłym zebranie kilkuset megabajtów takich informacji jednego dnia na jednym urządzeniu (może to być komputer, a nawet drukarka sieciowa). Kategoria ta obejmuje wszelkie operacje na obiektach. Zostanie tam odnotowana np. próba odczytania pliku. […]

Stellen Sie sich vor, Sie müssten wegen eines Computervirus, wegen eines entdeckten Einbruchs ins Computersystem oder einfach wegen eines Absturzes (Havarie) ihren Rechner ausschalten oder eines seiner Systemprogramme schließen. […]

Die sicherste sowie die meist empfohlene Lösung ist eine Neuinstallation (Wiederherstellung). Sie ist jedoch sehr arbeitsaufwendig. […]

Die andere Lösung ist, die Wiederherstellung des Computerzustands von vor der Modifizierung und das Installieren von funktionierenden Diensten von der Sicherungskopie. […]

In allen gegenwärtigen Betriebssystemen sind Überwachungsmechanismen eingebaut, mit deren Hilfe bestimmte Zugriffsversuche der Computernutzer protokolliert werden. In Windows-Systemen ist dafür der Sicherheitsprotokolldienst (Ereignisanzeige) verantwortlich. In älteren Windows-Systemen ist dieser Dienst benutzerdefiniert nicht eingeschaltet. […]

Die erste Kategorie ist die Überprüfung des Zugangs zu Objekten (Objektzugriffsereignisse). Das Einschalten dieser Kategorie ruft einen enormen Anstieg der Informationsmenge in den Dateien des Sicherheitsprotokolldienstes hervor. Nicht selten sammelt man so an einem Tag auf einem Gerät (Computer oder Netzwerkdrucker) hunderte von Megabytes an entsprechenden Informationen. Mithilfe dieser Kategorie können Sie Zugriffsversuche auf bestimmte Objekte auf einem Computer verfolgen. Dort werden z. B. Zugriffsversuche, bzw. Versuche eine Datei auszulesen, verzeichnet. […]