Zeitschrift: Bulletin Electrosuisse
Herausgeber: Electrosuisse, Verband für Elektro-, Energie- und Informationstechnik
Band: 99 (2008)
Heft: 5

Rubrik: Forum

Christian Studer

Security ist ein Prozess
La sécurité – un processus

Es wird viel über das Thema Security diskutiert und vor möglichen Gefahren gewarnt. Im Alltag läuft es darauf hinaus, hier mal ein Loch zu stopfen, da einen neuen Patch für eine aktuelle Signatur zu laden. Doch wer hat den Überblick, was wann wo und wie gemacht werden muss?

Um diesen Überblick über die Sicherheit in TCP/IP-Netzen zu haben, muss das Expertenwissen von verschiedenen Bereichen kombiniert werden. Deshalb muss das Thema Sicherheit als dauernder Prozess verstanden werden. Jede Änderung eines Parameters des Netzwerks kann sicherheitsrelevante Auswirkungen auf andere Komponenten oder das ganze Netz haben. Aus Sicht des Unternehmens ist es nicht wichtig, ob eine einzelne Komponente oder ein spezifischer Dienst verfügbar ist. Die Herausforderung besteht heute darin, Businessprozesse nachhaltig sicherstellen zu können. Ob dies durch geeignete Business-Process-Management-Software geschieht, welche diese Prozesse visualisieren und monitoren kann, oder durch andere, klar definierte Überwachungsmöglichkeiten, wird sich je nach Firmengrösse entsprechend unterscheiden. Wichtig ist, dass nicht nur einzelne Bereiche betrachtet werden, sondern das gesamte Umfeld. Oft denkt man an den Schutz vor Malware (Antiviren-Gateway), den Netzwerkzugangsschutz (Firewall, Authentifizierung und Autorisierung), an Notstromversorgung und Klimaanlage, an Datensicherung und Datenwiederherstellung oder auch an den Wireless-Zugangsschutz (WiFi, Bluetooth, ZigBee ...). Aber der mechanische Schutz der physikalischen Verbindungen (Kabel und Stecker), der Schutz der Spannungsversorgung (EMV-Schutzzonen BSZ 0-3), die Zugangskontrolle (Areal, Gebäude, Raum) oder das Sicherheitsbewusstsein der Mitarbeiter werden oft vergessen oder als nicht so wichtig betrachtet. Alle diese Punkte können jedoch einen Einfluss haben und müssen beachtet werden. Weiter sollten die Anforderungen an die Netzwerksicherheit in einer Security-Police festgehalten werden. Als Grundlage dafür gibt es die Norm ISO/IEC 17799:2000.

Sicherheit ist ein stetiger Prozess, und alle Netzwerkanpassungen und Änderungen haben einen Einfluss darauf. Diese sollten entsprechend geplant werden.

On parle beaucoup de la sécurité, on met en garde contre les dangers éventuels. Dans la pratique, cela se résout à boucher un trou par-ci, à charger un nouveau correctif pour une signature actuelle par-là. Mais qui a la vue d'ensemble, qui sait que faire où et quand?

Afin d'avoir la vue d'ensemble de la sécurité des réseaux TCP/IP, il est indispensable de combiner le savoir-faire d'experts de différents domaines. Aussi le sujet de la sécurité doit être considéré comme un processus permanent. Toute modification d'un paramètre du réseau peut avoir sur d'autres composants et sur tout le réseau des répercussions importantes du point de vue de la sécurité. Pour l'entreprise, peu importe qu'un composant isolé ou un service particulier soit disponible. Le défi consiste actuellement à pouvoir garantir durablement les processus commerciaux. Quant à savoir si cela sera réalisé au moyen d'un logiciel approprié de Business Process Management permettant de visualiser et de surveiller ces processus, ou par d'autres possibilités de surveillance clairement définies, cette question dépendra de la taille de l'entreprise. L'important est de ne pas considérer des domaines isolés, mais l'ensemble. On songe souvent à la protection contre les malwares (passerelles antivirus), à l'accès par le réseau (pare-feu, authentification et autorisation), à l'alimentation électrique de secours ou encore à la protection d'accès sans fil (WiFi, Bluetooth, ZigBee ...). Mais on oublie souvent aussi la protection mécanique des connexions physiques (câbles et fiches), de l'alimentation électrique (zones de protection CEM BSZ 0-3), le contrôle d'accès (terrain, bâtiment, local) ou la conscience de sécurité des collaborateurs, ou bien on ne leur attache pas tellement d'importance. Or tous ces points peuvent avoir une influence et il faut en tenir compte. En outre, il conviendrait de retenir dans une politique de sécurité les exigences posées à la sécurité des réseaux. Il y a comme base pour cela la norme ISO/CEI 17799:2000.

La sécurité est un processus permanent et toutes les adaptations et modifications de réseau ont une influence sur elle. Il convient donc de les planifier en conséquence.

Christian Studer ist Geschäftsführer der DDS NetCom AG, die Lösungen im Bereich Netzwerk und Sicherheit anbietet
Christian Studer est directeur de DDS NetCom AG qui propose des solutions dans le domaine réseaux et sécurité