14. tétel

I am an adviser (tanácsadó) of a network security firm. Your law firm (ügyvédi iroda) asked me to secure your IT system. Now, I would like to inform you about some security solutions. If you have any questions, please, do not hesitate to contact me.

First of all, I suggest using **secure passwords**. For example, you can use a whole sentence (egész mondat), or you have to use capitals, small letters, numbers or special characters. Another solution is using **strong random password**. In this case you will get a very difficult password with capitals, small letters and numbers (which you can’t memorise) by e-mail or on your mobile phone by SMS.

Secondly, if you don’t want others to see your files and folders you can give **file** and **folder permissions** (engedély) and you have to adjust **file level access management** (állományszintű jogosultság kezelés). Your files can be readable, erasable or editable or not. A file can be encrypted by a username and a password. So your law firm can **grant** (engedélyez) or **deny access** (megtagadja a hozzáférést**), allow** or **deny permissions**. (engedélyezi vagy megtagadja a jogosultságot)

Thirdly, I strongly advise you to use **firewall.** It is a **network security system** that monitors (figyeli) and controls the incoming and outgoing network traffic based on predetermined (előre meghatározott) security rules. A firewall makes a barrier (korlát) between a secure internal network and an untrusted (megbízhatatlan) outside network (for example the Internet). Firewalls are often categorized as either network firewalls or host-based (kliens-oldali) firewalls.

Network firewalls **filter traffic** between two or more networks; they are either software appliances (alkalmazás) running on general purpose (általános célú) hardware, or hardware-based firewall computer appliances.

Host-based firewalls provide a layer of software on a host that controls network traffic in and out of that single machine (gép). Firewall appliances may also offer (kínál) other functionality to the internal network they protect, such as acting (például úgy viselkedik, mint egy) as a DHCP or VPN server for that network.

Furthermore (továbbá), I advise you to create **virtual private network (VPN)**. A VPN enables (lehetővé teszi) users to send and receive data across shared or public networks. Applications running across the VPN benefit (hasznot húz) from the functionality, security, and management of the private network. A VPN is created by establishing (létrehoztak) a virtual point-to-point connection through the use of dedicated connections, virtual tunnelling (alagút) protocols, or **traffic encryption**.

What is a VPN?

If you have never heard of Virtual Private Networks or VPNs, you have come to the right place. A Virtual Private Network is a tool that creates a secure & encrypted connection between you and a remote server, the server then communicates with the internet on your behalf (te helyetted) keeping you anonymous (névtelen). VPN increases (növel) online privacy (titoktartás) by protecting your identity (személyazonosság), personal data, communications and other information from cyber criminals (bűnözők), ISPs (internetszolgáltató), surveillance agencies (felügyeleti irodák), and others. Only a VPN keeps your online activities private from Government Surveillance (kormányfelügyelet), ISP Monitoring and Cyber criminals. The remote server gives its IP address rather than revealing your real IP address. The best VPN providers offer online privacy for businesses, public Wi-Fi users, home users, online gamers. A VPN offers state of the art encryption which secures data by converting it into alpha-numeric code. Once the VPN encrypts data it can then only be decoded with a key, which is only available to the user. You can choose from the Windows, Android, iOS, and Mac VPNS to find the best provider for all your devices and operating systems. We can also offer leading VPN apps for both desktop & mobile devices. VPNs are also available over devices that are not directly compatible. You can configure the service over routers, Blackberry devices, Amazon Fire devices, PlayStation & Xbox consoles, Linux machines, streaming boxes (ROKU, Boxee etc.).

Finally, the fact (a tény az, hogy) is that you have a private network which consists of three main elements, a server, an office pc and an office laptop. If you are **outside the office** your remote computer can be connected to the private network. If you feel unsafe because of the Internet and you are afraid of stealing or modifying your data you only have to use a Secure VPN Tunnel to secure your IT System.