SPRÁVA FIREWALLŮ A ANTIVIROVÝCH SYSTÉMŮ VE SPOLEČNOSTI ORKLA FOODS INTERNATIONAL

Martin Kořínek

GUSEPPE A.S., Třída ČSA 449, 500 03 Hradec Králové, ČR, martin.korinek@guseppe.cz

Abstrakt
Příspěvek se snaží předložit některé zkušenosti se správou a rozšiřováním dvou bezpečnostních systémů – firewallů CheckPoint (FireWall-1 VPN-1 NG) a antivirových programů (F-Secure, ScanMail) v nadnárodní společnosti Orkla Foods International, která se v současnosti skládá z pěti firem (Rakousko, Polsko, Maďarsko, Rumunsko, Česká Republika). Rovněž se zaobírá výhodami a nevýhodami, které vznikly začleněním IT oddělení jednotlivých společností do jediného útvaru IT OFInt.

1. Struktura společnosti Orkla Foods International

Od minulého roku, kdy jsem referoval o společnosti Orkla Foods International (OFInt.) a především o Firewall Competence Center, došlo ke dvěma zásadním organizačním změnám:

1. OFInt. byla rozšířena o další společnost – rumunskou Orkla Foods.
2. IT oddělení jednotlivých společností přecházejí pod jediné vedení.

1.1 Rumunská Orkla Foods.

Rumunská společnost Orkla Foods se skládá ze dvou poboček, které jsou umístěny v Bukurešti a Craiové. Vedle těchto poboček má Orkla Foods Rumania čtyři sklady – Temešvár, Cluj, Bukurešť a Bacau. Společnost se zaměřuje na výrobu džemů a margarínů.

Začlenění společností znamenalo po stránce IT instalovat standardní softwarové systémy – Scala (účetní a informační systém), Lotus Mail (e-mailový a informační systém), F-Secure (antivirový systém) a v neposlední řadě nakonfigurovat firewall CheckPoint Firewall-1.

1.2 OFInt IT

V současné době je každé IT oddělení řízeno finančním ředitelem dané společnosti. Jednotlivá IT oddělení spolu, pochopitelně, spolupracují – především na standardizaci SW a HW vybavení.

Od konce minulého roku se vedou jednání směřující k tomu, aby jednotlivá IT oddělení spadala přímo pod jediné vedení, kterým by bylo IT OFInt. Těsně před schválením je SLA dohoda, mezi jednotlivými společnosti a IT OFInt., která specifikuje, jaké služby a v jakém časovém horizontu bude IT OFInt. „dodávat“ jednotlivým společnostem.

Managementu jednotlivých společností se tato struktura příliš nezamlouvá, neboť ztratí kontrolu (i finanční – rozpočtovou) nad svými IT odděleními. Na druhou stranu je zde objektivní tlak na to, aby se nutná standardizace (především některého SW, ale i HW) řídila z jednoho místa.

Přechodem jednotlivých IT oddělení pod IT OFInt. dojde také ke změně pracovních smluv jednotlivých IT pracovníků.

A jeden příklad neblahého dopadu těchto změn:
Management GUSEPPE se rozhodl, že jeden ze současných dvou pracovníků IT bude převeden do oddělení controlingu. Pojistil se, aby alespoň jeden IT pracovník zůstal pod vlivem GUSEPPE Pod IT OFInt. přejde pouze jeden zaměstnanec, který se na mezinárodní úrovni staral o firewally (Firewall Competence Center – FCC). Pochopitelnou reakcí ze strany IT OFInt. bylo, že s ohledem na časovou náročnost IT práce v GUSEPPE, odvolalo dosavadního člena FCC a nahradilo jej jiným pracovníkem (z Rumunska) a to přestože nový pracovník se musí vyškolit a s již značně rozsáhlým systémem se seznámit.

Přikládám větší část e-mailové korespondence:
Nejprve „suché“ konstatování (které, mimochodem, dostal jmenovaný pouze jako „na vědomí“)::

Hello Hans,
from my point of view we need:

- *overview about Checkpoint installations and software maintenace costs (valid from to)*
- *transfer of the firewall management console to Felix-Austria or Orkla Foods Romania. What is the best solution ? Please Note: the transfer will be done, because Martin in Czech will be the only one IT person in Czech because Dobros moved to Controlling. Martin allone can not handle all the IT-cases in Czech and for OFInt. This has nothing to do that let say, we were unhappy with Martin (this is not true, we are happy with Martin and he did an excellent job but we have to make strategical changes according to the ressources, we have).*
- *The strategy is that OFR (Deme and Giumi) will take over the responsibility for the whole OFInt. network (incl. ISP's, monitoring, new installations, costs, future strategy etc. etc.).*

These are only my points, which should be discussed with Deme and Giumi on Friday.
But once again, this should not be "small talk", it must be resulting in documentations, done from Deme and/or Giumi after the meeting.

Best regards,
Werner

A posléze pokus o vysvětlení:

Helo Martin,
yes I agree it's not a good international communication, but sorry I have very limited time.
As I wrote this is nothing against you or your work it's only reflecting the fact, that you are now alone in Guseppe/IT.

OFR in Craiova there are 2 in OFR and 1 in Topway. So we have there 3 persons and if one of them is out at least 2 are available. In your case, if you are away, nobody is there and Karel or Jiri will follow the SLA if something happens and we are getting in troubles.

I need you much more on this position to stabilize the IT operation in Guseppe as on the checkpoint firewall issue.

You will be satisfied in the future I will promise you,
and sorry for the short communication.

Best regards,
Werner

A verze pro management GUSEPPE:

About the firewall server. This is not a server, this is only a software management tool to be able to manage all of the firewalls from one centralized point. As now the situation is that only Martin Korinek is working for IT we cannot continue with this solution. As you know we cannot send Martin for urgent problems or bigger projects (Superfish in the future) away as we are not able to deliver the service for Guseppe as promised and described in the SLA.

Additional we have to find cost saving aspects to reach the financial goals. This issue will be much more time needed in the future (checking the WAN, negotations with suppliers, with Orkla etc etc) which can also not be handled from Martin, if Dobros will continue in IT.
This issue is only to be seen as a ***manpower ressource*** *problem. We only have ressources in OFR. Let's say in Craiova are situated 3 persons and additional 2 persons in Bucharest. We have some free ressources there. As the salaries in Romania are much more lower than in any other company in our division it makes no sence to reduce the personal because the possible gainings are not comparible to the losses of service.*

Summary:
What I can see, this change is absolutly not negative or bad for Guseppe (why ?, in the opposite you will have much more benefit from Martin, because he is not going to travel a lot in the future and he can give you more support). Anyway if OFInt is able to hold such competence within the divison, it doesn't matter where this service is situated, on the IT-side we are one unit.
And Martin has a big work and responsibility in front of him, much more than now. We like him very much and we wish him the best. As I wrote before this was a ressource problem, created from the changed situations (reduction of IT in Guseppe and increased needs due to the new IT-organization). And Martin is not loosing this experience, this knowledge is the basic in IT.

2. Firewall Competence Centre

2.1 Současný stav

Fiewall Competence Centre (FCC) je zodpovědné za správu a instalování firewallů CheckPoint Firewall-1 VPN-1 NG v rámci celé OFInt.

V současné době se jedná o tyto firewally:

Polsko

Firewall ve **Varšavě** (Compaq , Windows 2000 Server)
Firewall v **Kotlinu** (Compaq, Windows 2000 Server)

Rakousko

Firewall v **Mattersburgu** (Compaq, Windows 2000 Server)

Maďarsko

Fiewall v **Budapešti** (Compaq, Windows 2000 Server)

Česká Republika

Firewall v **Hradci Králové** (Compaq, Windows 2000 Server)
Management Console v **Hradci Králové** (Compaq, Windows 2000 Server)

Rumunsko

Firewall v **Bukurešti** (Compaq, Windows 2000 Server)
Firewall v **Craiové** (Compaq, Windows 2000 Server)
Firewall – sklad **Bukurešt** (NOKIA IP 71, update na NG)
Firewall – sklad **Temešvár** (NOKIA IP 71, update na NG)
Firewall – sklad **Cluj** (NOKIA IP 71, update na NG)
Firewall – sklad **Bacau** (NOKIA IP 71, update na NG)

V nejbližší době se připravují tyto změny:

- Instalování firewallu (NOKIA IP 71, update NG) v Rokytnici v Orlických horách. V současné době je zajištěno krytování mezi firewallem v Hradci Králové a routerem Cisco (série 2600) v Rokytnici v Orlických horách, kde je výrobní závod GUSEPPE.
- Upgrade všech firewallů a modulů na verzi (service pack) FP 3

2.2 Některé problémy

Během posledního roku jsme se opět potýkali s některými problémy. K těm výraznějším patřily:

- **Upgrade na verzi FP3**. Pro správný chod celého systému (11 firewallů řízených Management Consolí) je nutné, aby se s upgradem začalo právě na Management Consoli. Potíže byly spojené s tím, že CheckPoint přejmenoval některé moduly a u některých změnil jejich funkce. Po upgrade se „ztratily“ některé logy a změnily se parametry dvou objektů.
- **Upgrade firewallu v Oslo**. Pro komunikaci Domino serverů (Lotus Notes) je vytvořeno VPN propojení mezi firewallem v Rakousku a firewallem v Oslu (kde je umístěn nadřazený Lotus Server). Po provedení upgrade v Oslu přestalo toto VPN propojení fungovat. Po konzultaci a ověření parametrů obou objektů jsme zjistili, že upgrade pozměnil parametr VPN kryptování u objektu „non managemed firewall“ v obou lokalitách (Oslo, Rakousko).
- **Instalování firewallů NOKIA IP 71 pro sklady v Rumunsku**. Všechny 4 firewally pro sklady v Rumunsku se konfigurovaly v Hradci Králové, kde je umístěna Management Console. NOKIA IP 71 je hardwarové („routerové“) řešení (black box). Nejprve přes výslovné ubezpečení, že lze instalovat verzi NG Firewall-1 na NOKIA IP 71, jsme zjistili, že lze instalovat pouze verzi starší a to 4.6. Dále po testování jsme dospěli k názoru, že jedna NOKIA IP 71 byla nefunkční, nešlo nainstalovat poslední verzi firmware. Nic méně se nakonec podařilo všechny firewally zprovoznit a umístit na sklady. Později vyvstal požadavek na e-mail propojení skladů (původní požadavek byl jen na propojení na informační systém). Verze 4.6 ale umožňuje generovat toliko jedno VPN propojení. Naštěstí byla již k dispozici novější verze firmware, na kterou bylo možno nainstalovat verzi NG a vytvořit další VPN propojení.

3. Antivirové systémy

OFInt. používá na serverech a pracovních stanicích antivirový systém F-Secure. Pro virovou ochranu na manilovém serveru (Domino – Lotus Server) používá ScanMail.

3.1 F-Secure

Minulý rok došlo ke standardizaci nastavení F-Secure parametrů. V jednotlivých lokalitách si IT oddělení nejprve spravovalo F-Secure samo, což dokladuje následující stav:

Felix Austria – F-secure Administrator v4.04, maintains some policies and download updates on the server (BackWeb) every four hours and distribute it on all clients. The anti-virus installed is similar to the concept being recommended.
Recommended Changes: No major changes. Only upgrade the server to the latest version.

Felix Hungary - The current anti-virus solution in our company the FSecure software. It's installed on the client PC's. Time to time we receiving virus update from Mattersburg. I'm put it to a network folder and send a letter for the users that please doubleclick to the update file.
Arpad

- every pc has it's own local managed installation
- the updates are also made on every pc locally
- the software version is: 4.08.2170, AVP engine v.3.00, F-Prot engine v.3.06
george
Recommended Changes: Refrain from having Backweb on each client, inorder to lessen the internet traffic. The concept should be implemented ASAP.

Gusseppe - Hello Gerlie Ann! We use F-Secure 5.40 on all workstations and servers. We use "central management" with BackWeb. I use policy. I use standard but I had to change some parameters. For some users I had to switch off check the Excel file (only real time mode). I check the PC only one per day - at 1 PM, on servers at 4 AM.
Martin
Recommended Changes: No major changes, maybe only synchronize the policy, inorder that OFInt companies have common policies.

Kotlin – Hello, Today we using F-secure Antyvirus on workstations and servers but we don't use automaticly update policies for all workstations (some problems with Windows95). But we update manually - download virus definition from web site and save on server in public place after than inform users about possibilty update antivirus. But, In the future we will use full automaticly update policies
Best regards
RAFAL MIKOLAJCZYK
Recommended Changes: Implement the concept.

Orkla Foods Romania – the recommended solution is already tested and implemented on most of the clients (on the implementation process) and its running without problems.
Recommended Changes: Finalize the implementation.

Po této analýze doporučilo IT OFInt. následující nastavení (uvedeny jsou pouze změny oproti default nastavení):

F-Secure Management Agent
Change *Allow user to unload products* to *Not allowed* in order to prevent users to unload the antivirus service.

F-Secure Antivirus
In the **Visual** section change *Status Indicator* to *Disabled*. This will hide the icon in the system tray disabling user's direct access to the application settings.

In the **Real-Time Protection** section make the following changes:

- Set *Scan files* to *All files*
- Set *Action on infection* to *Disinfect Automaticaly*. This will be the default action whenever an infection will be detected; the user will not be prompted to select the action to be performed (default system option).
- Set *Scan inside archives* to *Enabled.*
- Go to **Action, Advanced – Actions Table** and in Table 0 change the *Secondary action* to *Delete Automaticaly*. In this case if disinfection fails the file will be permanently deleted to eliminate further infections risk.

Change the same settings for Manual Scanning.

These settings will propagate to all the clients wihtout the need for manual changing the settings for each client.

After all the settings are defined you can go to the right panel and check the *final* checkbox for some or all of the settings. This will disable the selected controls in the user interface. Any further changes will be done only by the administrator by changing the policy and distribute it to the users. Basically, the user will have no control over the antivirus settings. All of them will be administratively set and propagated to users through policies.

Vzhledem k automatické aktualizaci virové databáze a dennímu skenování všech počítačů nezaznamenalo GUSEPPE (naštěstí) žádný velký virový útok. Je to také tím, že nepoužíváme MS Outlook, ale důsledně jen Lotus Notes.

Menší problémy s chodem F-Secure lze popsat takto:

- **Zatuhnutí PC**. Při rezidentním skenování (real time) docházelo k velkému zpomalení až zatuhnutí některých PC. Po prozkoumání jsme zjistili, že se toto děje při práci s velkými Excel soubory (velikost nad 5 MB, výjimkou nejsou ani 30 MB soubory). Toto jsme odstranili tím, že jsme zakázali real time skenování Excel souborů.
- **Schedulování manuálního skenování**. Nejprve jsme nastavili manuální skenování (na Management Consoli) jen jednou denně po 15 minutách nečinnosti. Ale po rozdistribuování se počítače kontrolovaly vždy po 15 minutách nečinnosti a to vícekrát denně. Parametr v F-Secure zřejmě nepracoval správně. Proto jsme raději nastavili manuální skenování každý den ve 13:00, kdy je většina uživatelů na obědě.
- **Přejmenování PC**. Pakliže přejmenujeme PC, musíme přeinstalovat F-Secure, protože se toto nově pojmenované PC s Management Consolí nespojí, přestože je na PC korektně F-Secure nainstalovaný. Ale vzhledem k tomu, že instalování na klienty provádíme vzdáleně a PC nepřejmenováváme často, je toto nepodstatné.

3.2. ScanMail

Na jediném OFInt. Domino serveru (Lotus Notes) v Rakousku je nainstalovaný antivirový systém ScanMail. Slouží k rezidentní a manuální kontrole jak mailů tak i Notes databází.

Přestože se o ScanMail starají z IT z Rakouska, IT GUSEPPE má přístup jak k logům tak i (kupodivu?) k nastavení.

ScanMail od svého nasazení pracuje velmi spolehlivě a prozatím jsme nebyli vystaveni větší virové nákaze. Při pohledu do logů je však patrno, že každý den ScanMail objevuje virové útoky. Zajímavý je i TOP TEN žebříček – jak virů tak i uživatel.