

Who is reading my emails?

**//// TDP**

Václav Šamša  
TDP Ltd

# Who is reading my emails?



- I'm working with Novell products since 1987
- With Groupwise itself since WordPerfect Office 3.0
- Consultant and IS designer
- One of founding members of GroupWiseR
- Vaclav is beast from the east - Erno de Korte :-)
- [vsamsa@tdp.cz](mailto:vsamsa@tdp.cz), [www.groupwise.cz](http://www.groupwise.cz)



# Who is reading my emails?



## AGENDA

- Frightening story behind
- Customer questions thru the time
- Admin Attacks
- Trusted Applications
- Anivirus & AntiSPAM
- Protective measures
- What about Exchange?
- Conclusions

Who is reading my emails?

**//// TDP**

# Story

What is the right customer question?

And why is customer asking You?

...

# Who is reading my emails?



## Admin attacks:

- Password Change
  - Admin can change user password and log in as the user - this is common for all systems around the world
  - You can make it much more difficult by authentication against LDAP server with somebody else administering LDAP
  - If user detects password change without his or her previous request, it's definitely security incident
  - Unusable for hidden long time access to the user mailbox, useful when admin knows, what he/she is looking for

# Who is reading my emails?



## Admin attacks (cont):

- Backup
  - Admin can restore backup in different location and examine anything - this is common for all systems around the world
  - You can make it much more difficult if backup Admin is somebody else, using only GWTSA i.e.

# Who is reading my emails?



## Admin attacks (cont):

- Archives
  - Admin can dig data out of the archives if they are kept on the server (at user home directory i.e.)
  - Thanks to FID editor, Admin can bind archive to existing or new user by changing archive ID

# Who is reading my emails?



## Admin attacks (cont):

- DBCOPY
  - Admin can make once or periodically binary copy of any part of the running productional GW system - post offices and domains, and examine anything
  - There is no effective countermeasure against such attack, dbcopy is great and smart utility (many thanks to Tay Kratzer), it can even control the load by defining number of threads

# Who is reading my emails?



## Admin attacks (cont):

- Keylogger, user “help”
  - Admin can install keylogger on user PC and poll the password
  - Admin can ask user for password just to “help” with something
  - Very successful method, You can make it more difficult by combination of password changes, LDAP authentication (use bind, not compare) and logins audit (at LDAP side)

# Who is reading my emails?



## Trusted Application Attacks:

- GWAVA stuff
  - RETAIN - stores all metadata within SQL database, Admin can search thru all mailboxes
  - RELOAD - Admin can make copy like with DBCOPY
  - Recommendation
    - wait for protective measures slide
    - pray

# Who is reading my emails?



## Trusted Application Attacks:

- GWAVA stuff (cont)
  - REVEAL - realtime access to whole system, Reveal user (accountant i.e.) can search thru all mailboxes
  - VERTIGO - Admin can grant proxy access to any mailbox for anybody, for a while ...
  - Great tools, many thanks to Roel van Bueren
  - Recommendation - use Redline for auditing usage of REVEAL and VERTIGO

# Who is reading my emails?



## Trusted Application Attacks:

- Admin own stuff
  - Admin can develop own trusted application which can do anything You can imagine
  - Recommendation
    - audit list of trusted applications periodically
    - wait for protective measures slide
    - pray

# Who is reading my emails?



## Antivirus & AntiSPAM Attacks:

- Those apps are using trusted application key
- GWA4 scanner i.e. can copy all the messages (filtering available) to specified GW account - BlindCarbonCopy or Surveillance
- It's invisible for anybody, works on domains or access PO's directly like reveal i.e.
- Recommendation
  - audit setting periodically
  - wait for protective measures slide
  - pray

# Who is reading my emails?



## Protective measures:

- Requesting status tracking makes some scenarios risky for Admin (when using client on unread item)
- The only effective measure is to encrypt all email communication
- Except only lunch invitation etc
- Backup your keys (certificate) otherwise You lost access to all sent and received emails - forever!
- Note - with encryption, You can't use GW system global signature

# Who is reading my emails?



## Exchange:

- With exchange it's much more easier - Admin has access to all mailboxes by default
- Admin can grant access to any user to any mailbox just by assigning MAD rights - this assignment is invisible for user from Outlook and it may be granted to a group
- There are hundreds of applications for direct reading of Exchange Jet database and extract any messages, any mailbox to favourite .PST file (remember the story?)

# Who is reading my emails?



## Conclusions:

- It's like with safe deposits - there is nothing 100% secure, but ...
- GW requires lot of knowledge and efforts to get access to user data
- Exchange, Kerio etc are pretty easy - You can do it with standard administrative tools or available 3<sup>rd</sup> party utilities
- If security and privacy is crucial for You, GW is the right choice
- Check this: [www.novell.com/coolsolutions/feature/19518.html](http://www.novell.com/coolsolutions/feature/19518.html)
- That's all

Who is reading my emails?

**//// TDP**

Q&A

Thank You!