

IBM i Security Fundamentals

Annual Review Service



0300 124 0992 / info@chilli-it.co.uk

Chilli 

■ Overview

It has been said that IBM i is one of the most secure operating systems. Unfortunately this is rarely true; not because it isn't one of the most securable operating systems but because this security doesn't happen automatically. Someone has to configure it and regularly monitor it and this is where the problem lies. There are many good security products and tools designed to help keep your systems safe, but how good is your security if fundamental areas are overlooked?

To put it another way; is it enough to invest in tools like an ODBC exit point checker or Integrated File System virus checker when you may not know:

How many of your user profiles have a password that is the same as their user profile? Hackers like these types of profile, it's easier for them to guess passwords and log on.

“

IBM i is not
automatically secure -
it has to be
configured and
regularly monitored

How many of your user profiles are no longer needed and can be deleted? Hackers like these as well; the more users, the more attempts to sign on.

What capabilities your user profiles have? Hackers absolutely love powerful profiles, it allows them to do more damage. And don't believe that hackers are always strangers who have to penetrate network security before getting to your IBM i; sometimes they're our own employees, already working on the system, who by design or accident can cause us serious issues.

If the fundamentals aren't being addressed how can we say our systems are safe? A security fundamentals review from Chilli IT will go a long way to helping you establish either that your security is on the right path or you need to rethink how secure you are.



■ IBM i Fundamentals Review Service

We will provide a report and consultation outlining the state of fundamental security on your system and how any exposures can be exploited. We will help you understand what you need to be doing to improve the security of your system(s).

Operating system and PTF level

Information will be provided on your current OS level; how current it is and how long before it goes out of support. Your group PTFs will be reviewed to show how current they are.

Security system values

System values are configuration settings that apply across your entire IBM i system or partition. Numerous system values are either directly or indirectly security-relevant. For instance password related system values dictate how strong your users' passwords must be. The review will outline what your current settings are and how they differ from the recommended settings and can thus be exploited.

User profiles

Chilli's review will detail:

- 1 How many user profiles have default passwords (password is the same as the user profile) and how many are in an enabled status.
- 2 How many user profiles have not been used recently.
- 3 What special authorities are and how many user profiles may have special authorities that they don't need. For example the *ALLOBJ special authority allows a user to work with any object on the system regardless of the security placed on an individual object.
- 4 How many user profiles can be used by another user, i.e. profile hijacking.
- 5 Profile activation scheduling and profile expiration scheduling.
- 6 Password expiration and sign on control. The review will also advise on settings to automatically disable unused user profiles.

For more information get in touch with your Account Manager
0300 124 0992 / info@chilli-it.co.uk

Chilli

Auditing

Auditing is one of the best things you can do to control security. You can proactively detect security issues much quicker and easier; you can use it as a forensic tool when you suspect there have been security incidents and it can also be used to provide answers to a vast number of questions. For example you could use auditing to determine which users are using your sensitive database files.

Chilli will recommend the following auditing is switched on and how that information is captured and can be refined.

- Unsuccessful logins
- Object authorisation failures
- Commands ran by powerful users
- Amendments to user profiles
- Usage of sensitive system objects.

Transport Layer Security

Encryption of data travelling between system is a recommendation and Chilli advise that TLS is used for TCP/IP applications such as TELNET, FTP, SMTP, etc. Therefore the review will outline how Digital Certificate Manager can be used to generate certificates and keys to implement this functionality.

“

Auditing is one
of the best things you
can do to
control security





File shares

IBM i Netserver allows directories within the Integrated File System to be set up as file shares giving access to Windows or Linux clients as mapped drives or directories. This means those clients can access IBM i directories and files like any other type of Windows or Linux shared drive.

Without proper controls security can be compromised via the IFS and file shares. By allowing read access to sensitive information such as PDF invoices or sales files information can be stolen. Read/write access to sensitive information such as invoices or sales files allows that information to be corrupted or deleted.

The Integrated File System encompasses the /QSYS.LIB file system. This holds everything that makes up an IBM i system, most importantly the operating system. One of the biggest threats could be a ransomware encryption attack which may traverse the network via non-IBM i file shares and encrypt the IBM i operating system if the relevant Integrated File System directory ('/' root or '/QSYS.LIB') is shared for read and write.

This could render the system inoperable and user information inaccessible.

The security review would detail what Netserver shares have been set up and methods to secure them.

IP Interfaces and Ports

A part of the review we can install software to continually capture network interface information. Therefore you can see day by day what TCP/IP interfaces are communicating with the system; on which ports; how many times during each day the interface occurred and the direction of the traffic flow. This will help you determine if there is any suspicious network traffic.

For more information get in touch with your Account Manager
0300 124 0992 / info@chilli-it.co.uk

Chilli 

Trigger programs

A trigger program is a user-written (or application supplied) program that runs whenever an operation occurs on a database file. For example, you may have an orders file with a trigger on it so that whenever an order record is added to the file a program is called to print the order.

Trigger programs can be a way to introduce 'trojan horse' programs into the database. For example a database trigger program could check to see who is the initiating user. If the user is QSECOFR (very powerful profile) the trigger program could run a command to change a normal user profile to have very powerful special authorities.

TCP/IP servers

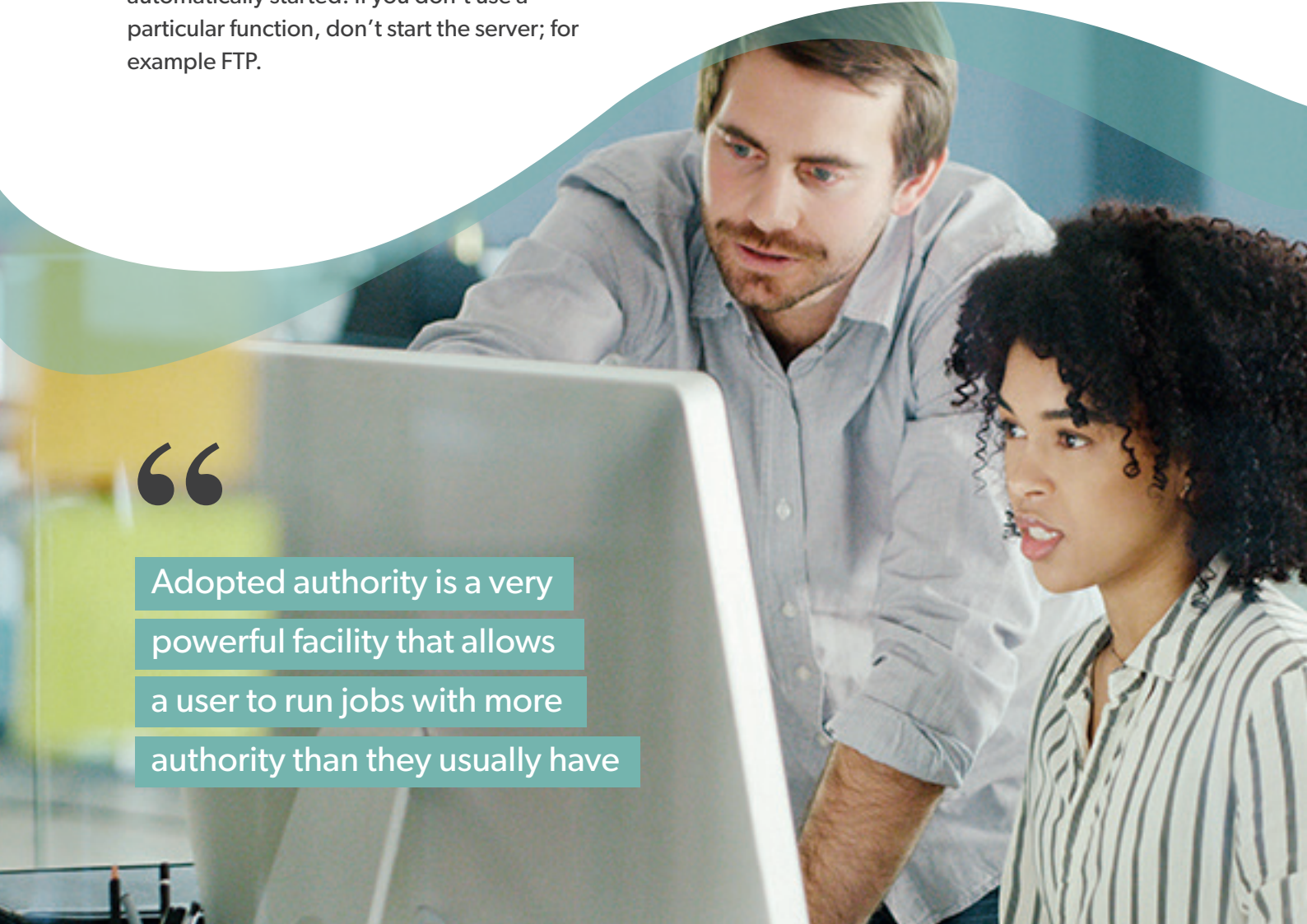
The review will outline which TCP/IP servers are automatically started. If you don't use a particular function, don't start the server; for example FTP.

Adopted Authority

Adopted authority is a very powerful facility that allows a user to run jobs with more authority than they usually have. When a program is compiled it can be set to run under the user profile of the person running the job or the program owner. If it is set to be the program owner and that profile is very powerful problems can arise. Adopted authority is a useful tool for controlling security but it can be exploited to give people more authority than they need.

Object authorities

We introduce object authorities and how they really are the only method of truly protecting your system. The review will cover the how users get authority to use objects based on the *PUBLIC setting.



“

Adopted authority is a very powerful facility that allows a user to run jobs with more authority than they usually have

ANNUAL REVIEW

£5,000

plus vat

Full IBM Fundamentals Report includes:

- ✓ Operating System & PTF Level
- ✓ IP Interfaces and Ports
- ✓ Security System Values
- ✓ Trigger Programs
- ✓ User Profiles
- ✓ TCP/IP Servers
- ✓ Auditing
- ✓ Adopted Authority
- ✓ Transport Layer Security
- ✓ Object Authorities
- ✓ File Shares

To discuss your options get in touch with your Account Manager
0300 124 0992 / info@chilli-it.co.uk