SRC
Secure Solutions

For more information visit our website using these links:

DATA ENCRYPTION

DATA COMPRESSION

SECURITY MANAGEMENT & COMPLIANCE

USER ENVIRONMENT MANAGEMENT

SYSTEM MONITORING

TWO FACTOR AUTHENTICATION

CLOUD BASED DEVICE ENCRYPTION

Find SRC on:

Twitter

You Tube

Facebook

Hello {FIRST_NAME}

It's great to see you back again in the exciting and dynamic world of IT security! As IT security threats grow like a pandemic and the race to halt this growth results in ever more sophistication in soft- and hardware no one can tell me that our profession is dull. I hope you enjoy reading this newsletter as much as we enjoy writing it.

A Virus on your IBM i?

A virus on my IBM i? You've got to be kidding! The operating system on the System i is designed in such a way that its supposed to be impossible to infect the system and do it harm. And yes that (in general) is correct.
But there are ways your IBM i system can be 'infected'.

The most well known occurrence is when the Integrated File System (IFS) is used as a network storage device. When Windows users are allowed to store files on the IFS there is a danger that infected files can be written to the system, either purposely or accidentally. But there is no immediate danger to the System i from these infected files. But when other users come to download an infected file the virus will be spread to other systems via the System i.

So, just like your desktops and Windows server systems, in order to be compliant (and safe!) if you use the IFS in this way you should run a regular virus scan on the IFS. To find out more about virus scanning read this document by Carol Woodbury and this one from RazLee.

While viruses are unknown on the IBM i Operating System there is still a danger of Trojans or 'altered' programs masquerading as IBM system software. For example someone wanting to read passwords could insert an Exit Program in the Telnet Exit Point, or standard IBM functions could be compromised by overwriting the 'innocent' program with malware using the same name. These dangers can also be reduced by a regular scan of your system using specialist software. For example the digital signature of an IBM program object can be checked. If a program has been illegally replaced, the scan will find it. For more information on this please contact SRC.

Hey I almost forgot, there is a FREE permanent licensed copy of

Anti Virus available to you now! Download it [here](#).

iSecurity

Phoenix Enterprises achieve hard-drive security with AlertBoot

Phoenix Enterprises at Rotherham, UK are a social enterprise, not for profit organisation with a team that is dedicated to helping unemployed people to return to work. Their aim is to increase employability and overcome social exclusion and since 1998 Phoenix has helped 37,741 people back into work. Currently they are helping someone back into work every two and a half hours of every working day.

As managing personal data is part of their business Phoenix has to comply with strict ICT Security regulations. One of these regulations is FIPS 140-2 for data protection. Phoenix is required to encrypt the hard-drives of all PCs and laptops in order to prevent data from falling into the wrong hands.

After scanning the market for full-disk encryption software their choice fell on AlertBoot Managed Device Security.

Phoenix
ENTERPRISES *The way to work*

AlertBoot is a cloud-based, managed suite of data security tools for individuals as well as big and small organizations. The scalable, cost-effective mobile security (smart phone, tablet) and computer disk encryption and management solution streamlines and simplifies data protection.

Centrally managed through a web based console, AlertBoot offers mobile device management, remote wipe & lock, device auditing and hard disk encryption managed services.

Phoenix's choice of AlertBoot was driven by the ease of use and the powerful cloud based management system, which allows the administrator to manage devices from any location.

You can read more about AlertBoot [here](#).

Contact us by [mail](#) or call us on +31(0)205036001.

AlertBoot™

SecureZIP successes

The last quarter has seen two major successes for SecureZIP and the establishment of SecureZIP as an industry standard within the pension and insurance branches.

Under pressure from a Dutch regulatory organisation to encrypt sensitive data at rest and in transit, one of The Netherlands largest pension service providers has deployed SecureZIP for Windows Server to encrypt and protect payment data files. The encryption standards offered in SecureZIP comply to the regulators requirements and its ease of use meant that implementation was a matter of just a few hours work. As PKI is incorporated in SecureZIP the company can easily combine with or replace passwords with asynchronous keys without changing the software.

Another recent success is the installation of SecureZIP for Windows Desktop at the Netherlands HQ of one of the worlds largest insurers. Here SecureZIP is used to automatically encrypt and compress emails sent using MS Outlook. Again its easy of use and quick deployment mean that the user was up and running on a multitude of desktops in a matter of hours.

You can find out more about SecureZIP here.

SecureZIP®

Rising competition!

Or "Imitation is the sincerest form of flattery".

SRC always seems to find a healthy niche. In the late 80's we specialised in IT communications, in the 90's EDI was our main game. Starting in the 'noughties' and going through the second decade of the 21st century we specialise in IT security. In the beginning it was a lonely road. Financial institutions of course have long seen IT security as the highest priority, but it still seems that it takes regulations and revelations (of data breaches) to hammer home the need for continual maintenance of systems to keep your data safe. Until quite recently that is. With the recent uncovering of data acquisition by the NSA and the increasing sophistication of hackers, with commercial search engines such as Google collecting and marketing your on-line behaviour. Now even in The Benelux, IT security has become a primary issue at most organisations and we at SRC are enjoying a busy time.

Now of course other IT suppliers are seeing the IT Security market as the next big opportunity and are becoming IT security specialists. So welcome on board colleagues! We take it as a compliment.

By Stephen R. Cheney

Deep Dive Security Training for IBMi

January 14 and 15, 2014, Security expert Carol Woodbury* presented a live, comprehensive training for IBM i Security.

The training course was well attended and Carol Woodbury delivered her knowledge to a keen audience.

This training will be repeated at the end of this year followed by an advanced section which will be offered to attendees of the first deep dive.

Reserve a space!
If you are interested in receiving information about the next Deep Dive please contact us here.

* Carol Woodbury is the former i Series Security Architect and Chief Engineering Manager for IBM in Rochester, MN; as well as author of the new book "IBM i Security: Administration & Compliance," award winning speaker on the topic of security, Certified in Risk and Information Systems Control (CRISC) and the Co-founder, President and CTO of SkyView Partners Inc.

SRC Secure Solutions bv
Wolfert van Borsselenweg 95
1181 PJ Amstelveen, - -
NL