The Encryption Dance

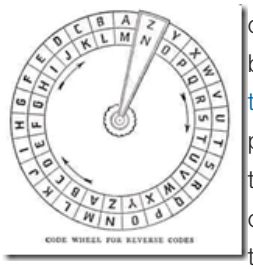
Peter Silva, 2009-14-08

S-s-s-s A-a-a-a F-f-f-f E-e-e-e T-t-t-t Y-y-y-y

You can make the Big S while you sing along.*

> Data goes where it wants to, It can leave your trace behind.
> Cause the web don't care and if it don't care, Well it's exposing time.
> I say, data can go where it wants to, A place where they will never find.
> And we can act like we come from NSA, Leave the eavesdroppers far behind.
> And we encrypt. Those things.
>
> We can surf where we want to, Data's masked and so am I
> And we can hide real neat from our hats to our feet,
> And surprise 'em with a 'Ha Ha' cry.
> Say, they can crack if they want to, if they don't somebody will.
> And if they do break in, the data is encrypted
> And they'll look like an imbecile.
>
> I say, we got data, we got data, Everything's in our control
> We got data, we got data, encrypting it wall to wall
> We got data, we got data, everyone check their systems.
> We got data, we got data, everyone's taking a chance
> Encryption Dance.

Encryption is a key element in security – both for data in transit and data at rest. It doesn't necessarily need to be highly sensitive data either. Just something you want to keep secret. I've written about encryption a few times, especially in



context surrounding high profile breaches like TJX and Heartland since both those might have been avoided if the data was encrypted. It's not as simple as the lyrics depict as Lori points out in this blog. Sure, there is SSL, HTTPS, IPSec and encrypted drives but it's difficult to encrypt every piece of data, especially for the enterprise. In fact, there's probably some data that doesn't need to be encrypted. Which is where a Access Control Policy can come into play. Depending on the context of the user/device, remote and mobile workers should be connecting via an encrypted tunnel using your VPN – that's a no brainer. Depending on the host inspection check, your policy might only allow access to certain resources depending on the device's posture and hopefully all that traffic is encrypted. Internal LAN's are no longer the 'safe haven' that they used to be. Partner's, contractor's and even unauthorized employees might have visibility to certain restricted information. Here again, a policy could be enforced to first, restrict access to certain areas of your network (which many do already) and second, if an authorized employee is grabbing sensitive data, why not encrypt that specific file transmission even on the internal network to thwart any prying eyes or sniffing agents.

As for PCI, there's already plenty of articles and opinions about it's current state and effectiveness so I won't dive in here. What I will point out is an upcoming deadline that many might be unaware of: The unattended, PIN entry, Point-of-Sale devices. While the deadline for PCI-DSS has passed, the deadline for PA-DSS entry terminals is next year – July 2010. That means that most gas station pumps that you use your debit with, are unencrypted today. There will be a mad rush next year for Fuel Retailers to either deploy an encrypted PCI-compliant PIN entry device inside or an encrypted keypad outside.

Finally, we continue to see data exposures due to stolen or lost laptops. Here again, depending on your policy, the type of user/device and information accessed (plus other criteria) encrypting the drive to protect against inadvertent exposure is certainly a good idea – along with strict and potential severe consequences if someone does not comply.

ps

*Sung to the tune '***Safety Dance***' by Men Without Hats.

#5 out of 26 Short Topics About Security

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com