Issue 2 - April 2013

The blackfoot Quarterly

ADVISE >

ASSESS >

ASSURE >

Welcome

Hello and welcome to the Spring 2013 Blackfoot newsletter. Christmas and New Year seem long forgotten already, and we're now in a frozen Spring; where does time fly?

In this issue we bring you up to date with the changes we know of in the year so far, as well as discussing a Microsoft Windows XP issue you should have already addressed. We also touch on the increasing importance of Application Security in today's environment.

So let's delve straight into it with a thought from our CEO Matthew Tyler.

Last year we said goodbye to a number of high street friends. This year is looking like a year of rapid change and the adoption of new technologies, ranging from Mobile payments through to omnichannel. The iPhone 3 was only launched in June 2009, so innovation is coming thick and fast as businesses compete for their market share.

Just what the future of retail looks like is a heavily debated topic. Are retail parks the future, with small independent retailers on the high street? Internet and mobile shopping sales continue to rise and click n' collect is becoming more and more common for electricals, clothing and food shopping. However, more stringent regulation is looming and changes to data protection and a focus on cyber security mean that you need to think before you leap. The benefit of having clients who are growing at double digit rates, and others who are struggling with like for like performances, gives us the ability to actively keep a view on all of these challenges. During our 2013 newsletters we will also be sharing some of our insights into what's coming down the pipe, what works and what doesn't.

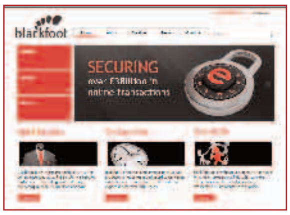
We see the next two years brimming with so many opportunities that there are just too many to mention. Watch this space.

Matthew Tyler
Blackfoot CEO

Quarterly Review

There has been a flurry of activity at the PCI Security Standards Council, and they published several documents as a result of the Special Interest Groups running last year. You now have PCI DSS E-Commerce Security Guidelines, PCI DSS Cloud Computing Guidelines and the newly released Mobile Payments Acceptance Guidance for Merchants. All three documents can be found on the PCI Security Standards Council website at www.pcisecuritystandards.org. Worthy of particular mention is the E-Commerce Security Guidelines that highlights OWASP, who provide a wide resource of training material and information on web application security. Our very own Colin Watson is on the OWASP global industry committee. He wrote the Cornucopia guide mentioned in the document – so well worth looking into it on OWASP website www.owasp.org or getting in touch if you'd like any more information.

The Information Commissioner has been talking about the potential EU data protection reforms. They have produced an updated analysis paper covering each article and their thoughts on it. This can be found at www.ico.gov.uk. Last year Blackfoot published a white paper on the impact of the new data protection regulation, which you can find on our website at http://www.blackfootuk.com/common/pdfs/whitepaper.pdf



In December we made you aware of an extremely concerning piece of malware aimed at retail clients called Dexter. It was active before the holiday period to pick up as much card data as possible. As this is an ongoing threat, please keep checking for this malware until your vendors make you aware of a patch to remediate the exploit. You can find the alert on our website at http://www.blackfootuk.com/common/pdfs/Blackfoot_Newsflash_Dec12.pdf

Last month Microsoft released an out-of-band security release for Internet Explorer and Oracle released an update for Java run time. Both are high priority patches so you should have installed these if you run them. You can find our note on these issues on our website at http://www.blackfootuk.com/common/pdfs/Blackfoot_Newsflash_Jan13.pdf

Articles

Many businesses still have tills or office networks running Windows XP and there is a significant deadline looming that you are hopefully aware of. Support for Windows XP and Office 2003 ends on 8th April 2014. At time of writing that is 13 months or 54 weeks away. Seems a while away but what if we say 386 days? Ok, how about 269 working days? Does that still sound a lot? No, we didn't think so either.

Do you remember the last time you upgraded your till computers, or office network or both? From business case to deployment, how long did it take to complete? 18 months if you were quick and it went smoothly? A large network may have taken 24 months or more. Time is running out if you haven't started planning for this and still use XP.

So firstly why is this happening and what is the definition of support? Back in 2002 (when the Euro was born, Sarbanes-Oxley Act 2002 was passed and the first camera phones were sold in the USA), Microsoft advised that they were going to be more transparent and introduce a formal lifecycle process for their products. In total you would have 10 years of support split by 5 years mainstream support and 5 years extended support. So XP and Office 2003 are out of time. Microsoft classifies support as security updates, non-security hot fixes and any free or paid support. The biggest risk to you is the security updates you receive at least monthly will cease, leaving you with unfixable holes in your network. Other issues you may encounter is software that will be unlikely to run on XP, as the vendors are not obliged to support it. At the same time, older versions of applications you use may not run on Windows 7 or 8 if they have not been built to.

As you can see it will create significant challenges for businesses and if you are one of them now is the time to act.

As we have mentioned applications may not run on different OS versions it leads us neatly into our next subject of Application Security.

Blackfoot advocates having application security as part of your multi layered security approach. You can try to secure your network as much as possible but what happens when somebody gets in? Issues with zero day vulnerability, or somebody opens an email with an unknown attachment and all the security in the world may not help you. So build your applications with security in mind. Put it at the front of your requirements along with functionality and user interface. After all, if somebody does breach your network they can try to access your data, but a secure application will dramatically reduce the risk of anything meaningful being lost.

So carry out a code review against established industry best practice, and develop a secure software development lifecycle. For those of you who develop your own applications it will take time to introduce and establish but we can help you with this. Stop being reactive and reduce your reliance on penetration testing finding holes for you to fix. It has to better and more cost effective to be proactive and build your applications securely from the ground up.

That is all for this edition of the newsletter. Keep a look out for the summer edition hitting your mailbox in June.