Unicorns in the Wild – Information Security Skills and how to achieve them

Posted on **July 27,2017** by **lynx**

Everyone talks about information security, countering „cyber“ threats, endless feats of hackers gone wrong/wild, and more epic stories. Once you have realised that you are reading the news and not a script for a TV series, you are left with one question: What are information security skills? The next question will probably be: How do you train to be „information secure“? Let's take a look at possible answers.

First of all, yes, you can study information security or security-related topics. Universities, schools, and companies offer lectures, training, exercises, etc. Great. However it may not help you right away. We talked with top quality head hunters from a nameless big corporation. When they look for infosec specialists, they filter for anyone having worked in three different fields related to computer science (applied or otherwise) for at least two to three years respectively. Tunnel vision is not what you want when dealing with a complex infrastructure of hardware and software, some under your control, some parts belonging to someone else. One of the best combinations is system administration, software development, and support (the level is not important, but you have to talk to actual people about actual IT problems).

Once upon a time system administrators were generalists. Decades ago your first career move into this field was answering yes to the question if there's someone around who knows computers. It's still true, only the question also covers Wi-Fi, networks in general, apps, hand-held devices, TV sets, refrigerators, washing machines, coffee machines, vending machines, and almost everything that need electric power and connects to some network. Dealing with this computing stuff gives you a lot of insight into how systems interact, what goes wrong (things will go wrong, trust me, if in doubt look up the meme „down, not across“), how you can fix things, and what things definitely cannot be fixed. You also get your daily dose of coding since no system administrator can survive without scripting things – also known as orchestration or automation, thanks to the cloud gods who invented *devops*.

Software developers learn how to solve problems by using the programming language of the day. It really doesn't matter where to begin, as with system administration. Since there exists no general purpose computer or operating system to solve every problem on the planet, there is also no single programming language fit for all purposes. Make sure you understand what kinds of code there are. Having a peek at the processor level doesn't hurt. Try to understand the ecosystems your software project lives in. There is a plethora of computing platforms out there. Try to understand the reason for their existence, and all the interactions they have with the actual hardware that runs the code. As with system administration things will inevitably go wrong from time to time. Make sure your code can handle the real world – always.

So far we have covered hardware and software. Now for the most important aspect of the information security world: human interaction. All support staff gets more interaction than they can handle, at times. You cannot understand social engineering and how adversaries target the human element of the digital infrastructure if you haven't experience communication. Support staff shares major problems with system administrators and software developer: misunderstandings, lack of information, working with hypotheses, asking countless questions to get to the crucial information, report containing wrong information, and much more. Dealing with these issues in real-time is a challenge. It will give you a lot of insight into how small problems can turn into big ones.

If you are wondering which way to go, chances are that you already experienced a part of the disciplines described in this article. Provided you still want to deal with information security problems, which can be very frustrating and impossible to solve, you just need to gain more insight into the fields you haven't got into yet. It's not easy, but few digital job are. This is also why we have problems answering the question to who attends DeepSec. We aim for the mix of sysadmins, devops, developers, infosec experts, CEOs, CTOs, auditors, architects, and users. You need to see the horizon in order to see the storms coming. And unicorns can't swim.

Posted in:Discussion,High Entropy,Security | Tagged:Education,Mindset,Security,Training | With 0 comments