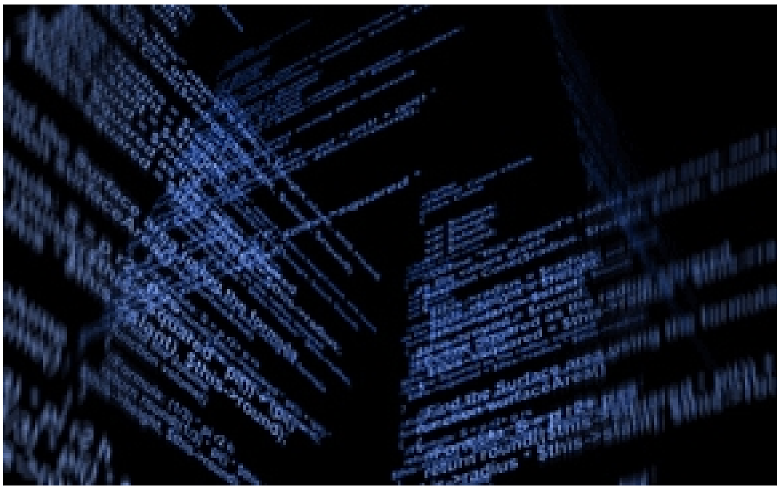
Dispruptive Data Security Key to Outwitting Hackers It is now widely accepted that the enterprise will be subjected to and may even succumb to cyber attack and yet we continue to rely upon a defensive security strategy. A far more effective way to combat the threat is to focus on disrupting the attack while keeping data safe. This article contains some practical do's and don'ts to help the enteprise transition to a data-centric strategy.



Enterprises need to move towards a data-centric disruptive security strategy given the inevitability of network compromise. The continued emphasis on network security solutions is out-of-step with the changing nature of threats, with attackers increasingly utilising automatic probing, botnets and malware to detect and exploit network weaknesses. By assuming a position of compromise the organisation can focus security resource on strategies such as disruptive data that uses dummy data repositories or bait records to automatically trigger alerts. This subterfuge buys the organisation the time needed to both respond and protect critical data.

To date, many organisations have sought to defend the network using a combination of defence-in-depth and point solution systems to sweep the network and feed a SIEM system. However, as data generation increases, collating and applying intelligence to interpret the relevance of these reports is becoming more difficult. In addition, the attacker is now able to draw on a far wider pool of resources and strategies to infiltrate the network, making the probability of a successful breach far higher.

Once inside the system, there is often little to prevent the attacker from acquiring prized data assets as most security spend is dedicated to prevention rather than protection. In contrast, an effective data protection strategy employs data encryption, multi-factor authentication, and data deidentification procedures as well as data subterfuge practices, to secure databases and access mechanisms. Regularly tested and audited, this level of data protection ensures that the lifeblood of the business – data – is kept safe from unauthorised access.

DO

- Anticipate further growth in sensitive corporate data and accept the prospect of an attack. Evaluate and record risk in a breach risk register

- Carry out an enterprise-wide assessment of data assets and record the information lifecycle process to determine how data will be handled from creation to destruction

- Make provisions for securing valuable data assets. Is sensitive data encrypted in transit as well as at rest? Is access restricted according to role? Who has responsibility for assigning or rescinding access? Consider key management and ensure keys are not stored in the same location.

- Obfuscate data through the use of mechanisms such as dummy data, bait records, and network segregation

DON'T

- Rely on network systems to give real time intelligence. As the amount of data the organisation processes over time grows, this will become cost prohibitive and burdensome. Information from point systems should be seen as supplementary information useful for monitoring traffic or investigations but should not be relied upon to stop an attack

- Confuse compliance with data security. Regulatory requirements should be seen as a generic bare minimum requirement and tailor the data protection policy to meet business requirements. Prevent security mechanisms from obstructing workflow by making them relevant and workable

- Make the assumption technology is more effective than people and process. There is no substitute for a meaningful enterprise-wide policy that is consistently applied by all personnel. Attacks will infiltrate the business. Accepting that as a fact may sound daunting but it can also be empowering, provided you know where to focus your efforts. Targeted attacks use advanced evasive actions, as the attacker wishes to operate discreetly to extract data, often amongst the noise of daily network business activities. Disrupting that activity by confusing the attacker, laying false trails and using segregation to protect the data 'crown jewels' has to be the way forward.

James Henry is Consulting Practice Manager, Auriga