Question

David Doe is a network administrator for the ABC Company. David is passed over for promotion three times. He is quite vocal in his dissatisfaction with this situation. In fact, he begins to express negative opinions about the organization in general. Eventually, David quits and begins his own consulting business. Six months after David's departure, it is discovered that a good deal of the ABC Company's research has suddenly been duplicated by a competitor. Executives at ABC suspect that David Doe has done some consulting work for this competitor and may have passed on sensitive data. However, in the interim since David left, his computer has been formatted and reassigned to another person. ABC has no evidence that David Doe did anything wrong.

What steps might have been taken to detect David's alleged industrial espionage?

What steps might have been taken to prevent his perpetrating such an offense?

Answers

Anonymous answered this
9 answers

It is very difficult task to detect,To detect, there are requirement of some security tools. Level of security depends on importance of the data.

Comprehensive protection of the IT infrastructure entails the use of automated modules for risk identification, focusing on six fields of application:

- The evaluation of log data from various sources as well as risk and threat data, with the aim of obtaining solid security information enabling rapid response to security incidents and pertinent compliance reports (Security Information and Event Management or SIEM).
- The detection of dangerous malware, anomalies and other risks in the network traffic by means of signatureand behaviour-based detection engines (Advanced Cyber Intrusion Detection or ACID).
- The collection, analysis and correlation of server and client logs and the immediate alerting and response as soon as attacks, misuse or errors are detected. The file integrity of local systems must be checked, and rootkits such as hidden attacks, trojans and viruses must be identified on the basis of system changes (Host-based Intrusion Detection or HIDS).
- A 360-degree overview of potential security vulnerabilities in operating systems and application software, and the monitoring of all data flows on the network anomalies (Vulnerability Assessment or VAS).
- The detection of advanced malware previously undiscovered by conventional security measures, including advanced persistent threat (APT) systems (Advanced Email Threat Detection or AETD).
- Automatic monitoring of compliance regulations and the immediate reporting of breaches to minimise compliance risks (Software Compliance or SoCo).

Was this answer helpful? 0 3

More Answers

Anonymous answered this
2,113 answers

1) Answer: -

In the given scenario, the company could have taken the following steps to detect David's Doe alleged industrial espionage:

- Check David's email to see if he attached or copied any sensitive data to an email he sent out to others.
- See if David uses apps and accesses data from the cloud that he shouldn't be accessing
- Check server logs to see what information David is accessing
- Check to see if David is using a remote server during off-hours
- Having a monitoring system is key to ensuring compliance and managing employee accounts that have access to sensitive data. An effective monitoring system will allow you to track, log and record account activity and create alerts to allow for a quick response when suspicious activity is detected. For example, multiple failed access attempts or bulk file copying may signal that a disgruntled or greedy employee is attempting to access the network in a malicious manner.
- Monitor user behavior and identify any unusual patterns.

2) Answer: -

The following steps can be included to prevent his perpetrating such an offense:

Identify Your Companies Trade Secrets: By properly evaluating their intellectual property, firms will be more able to establish priorities and allocate security resources to better protect their most vital secrets.

Identify the Threats: The largest threat could come from competitors, visitors, customers, business partners, hackers, activist groups, and even foreign national governments.

Ensure Physical Security: Firms should ensure the physical security of their offices, equipment, and infrastructure. This means setting up surveillance systems, securing entry points, and hiring or contracting specialized personnel. It is particularly important that firms identify the most sensitive information and facilities and ensure that these are given extra layers of protection.

Establish Policies for Controlling Information: Firms should establish policies on what information employees can share inside and outside the workplace. They should also establish procedures for the control, reproduction, and storage of sensitive data.

Train the Workforce: Firms should conduct periodic training and awareness campaigns to inform employees about the threat of industrial espionage and the importance of information security. Employees should understand that the threat of espionage is internal as well as external. As such, they should instruct workers on the correct procedures for identifying and reporting suspicious activity.

Compartmentalize Information: Firms should put in place policies to segregate which employees have access to which information, with special attention given to those employees who have access to a company's most vital trade secrets.

Conduct Background Checks and Monitoring: Firms should conduct background checks on all employees with access to sensitive data. This may even include often-overlooked individuals such as janitors, caterers, and groundkeepers. Specifically, firms should attempt to identify any possible factors that could make a particular worker more prone to illegally disclosing information.

Was this answer helpful? 0 0

Practice with similar questions

Q: David Doe is a network administrator for the ABC Company. Davidis passed over for promotion three times. He is quite vocal in hisdissatisfaction with this situation. In fact, he begins to expressnegative opinions about the organization in general. Eventually,David quits and begins his own consulting business. Six monthsafter David's departure, it is discovered that a good deal of theABC Company's research has suddenly been duplicated by acompeti...

A: See answer

Q: David Doe is a network administrator for the ABC Company. Davidis passed over for promotion three times. He is quite vocal in hisdissatisfaction with this situation. In fact, he begins to expressnegative opinions about the organization in general. Eventually,David quits and begins his own consulting business. Six monthsafter David's departure, it is discovered that a good deal of theABC Company's research has suddenly been duplicated by acompeti...

A: See answer

Show more

Questions viewed by other students

Q: David Doe is a networkadministrator for the ABC Company. David is passed over forpromotion three times. He is quite vocal in his dissatisfactionwith this situation. In fact, he begins to express negativeopinions about the organization in general. Eventually, David quitsand begins his own consulting business. Six months after David'sdeparture, it is discovered that a good deal of the ABC Company'sresearch has suddenly been duplicated by a competit...

A: See answer

Q: David Doe is a network administrator for ABC Company. David is passed over for promotion three times. He is quite vocalin his dissatisfaction with this situation. In fact, hebegins to express negative opinions about the organization ingeneral. Eventually, David quits and begins his ownconsulting business. Six months after David's departure, itis discovered that a good deal of the ABC Company's research hassuddenly been duplicated by a competit...

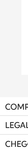
A: See answer 100% (1 rating)

Show more

My Textbook Solutions

Classical Electrodynamics

Solutions →



The Legal and Regulatory Environment of Busin...

Solutions →

View all solutions