

Incident report analysis - Example

This morning, an intern reported to the IT department that she was unable log in to her internal network account. Access logs indicate that her access has been actively accessing records in the customer database, even the she is locked out of that account. The intern indicated that she received email this morning asking her to go to an external website to log in with internal network credentials to retrieve a message. We believe this is the method used by a malicious actor to gain access to our network and customer database. A couple of other employees have noticed that several customer cords are either missing or contain incorrect data. It appears that not was customer data exposed to a malicious actor, but that some data we deleted or manipulated as well. Identify The incident management team audited the systems, devices, and access policies involved in the attack to identify the gaps in security. The team that an intern's login and password were obtained by a malicious attack used to access data from our customer database. Upon initial review, it appears that some customer data was deleted from the database.	ount ugh an ner stomer mer only
has been actively accessing records in the customer database, even the she is locked out of that account. The intern indicated that she received email this morning asking her to go to an external website to log in with internal network credentials to retrieve a message. We believe this is the method used by a malicious actor to gain access to our network and cut database. A couple of other employees have noticed that several custor records are either missing or contain incorrect data. It appears that not was customer data exposed to a malicious actor, but that some data we deleted or manipulated as well. Identify The incident management team audited the systems, devices, and accepolicies involved in the attack to identify the gaps in security. The team that an intern's login and password were obtained by a malicious attack used to access data from our customer database. Upon initial review, it	ugh an ner stomer mer only
she is locked out of that account. The intern indicated that she received email this morning asking her to go to an external website to log in with internal network credentials to retrieve a message. We believe this is the method used by a malicious actor to gain access to our network and cut database. A couple of other employees have noticed that several custor records are either missing or contain incorrect data. It appears that not was customer data exposed to a malicious actor, but that some data we deleted or manipulated as well. Identify The incident management team audited the systems, devices, and accepolicies involved in the attack to identify the gaps in security. The team that an intern's login and password were obtained by a malicious attack used to access data from our customer database. Upon initial review, it	an ner stomer mer only
email this morning asking her to go to an external website to log in with internal network credentials to retrieve a message. We believe this is the method used by a malicious actor to gain access to our network and cut database. A couple of other employees have noticed that several custor records are either missing or contain incorrect data. It appears that not was customer data exposed to a malicious actor, but that some data was deleted or manipulated as well. Identify The incident management team audited the systems, devices, and acce policies involved in the attack to identify the gaps in security. The team that an intern's login and password were obtained by a malicious attack used to access data from our customer database. Upon initial review, it	ner e stomer mer only
internal network credentials to retrieve a message. We believe this is the method used by a malicious actor to gain access to our network and cut database. A couple of other employees have noticed that several custor records are either missing or contain incorrect data. It appears that not was customer data exposed to a malicious actor, but that some data was deleted or manipulated as well. Identify The incident management team audited the systems, devices, and acce policies involved in the attack to identify the gaps in security. The team that an intern's login and password were obtained by a malicious attack used to access data from our customer database. Upon initial review, it	e stomer mer only
method used by a malicious actor to gain access to our network and cut database. A couple of other employees have noticed that several custor records are either missing or contain incorrect data. It appears that not was customer data exposed to a malicious actor, but that some data was deleted or manipulated as well. Identify The incident management team audited the systems, devices, and acce policies involved in the attack to identify the gaps in security. The team that an intern's login and password were obtained by a malicious attack used to access data from our customer database. Upon initial review, it	stomer ner only
database. A couple of other employees have noticed that several custor records are either missing or contain incorrect data. It appears that not was customer data exposed to a malicious actor, but that some data was deleted or manipulated as well. Identify The incident management team audited the systems, devices, and acce policies involved in the attack to identify the gaps in security. The team that an intern's login and password were obtained by a malicious attack used to access data from our customer database. Upon initial review, it	ner only
records are either missing or contain incorrect data. It appears that not was customer data exposed to a malicious actor, but that some data was deleted or manipulated as well. Identify The incident management team audited the systems, devices, and acce policies involved in the attack to identify the gaps in security. The team that an intern's login and password were obtained by a malicious attack used to access data from our customer database. Upon initial review, it	only
was customer data exposed to a malicious actor, but that some data was deleted or manipulated as well. Identify The incident management team audited the systems, devices, and accepolicies involved in the attack to identify the gaps in security. The team that an intern's login and password were obtained by a malicious attack used to access data from our customer database. Upon initial review, it	-
Identify The incident management team audited the systems, devices, and accepolicies involved in the attack to identify the gaps in security. The team that an intern's login and password were obtained by a malicious attack used to access data from our customer database. Upon initial review, it	s
Identify The incident management team audited the systems, devices, and accepolicies involved in the attack to identify the gaps in security. The team that an intern's login and password were obtained by a malicious attack used to access data from our customer database. Upon initial review, it	_
policies involved in the attack to identify the gaps in security. The team that an intern's login and password were obtained by a malicious attack used to access data from our customer database. Upon initial review, it	
that an intern's login and password were obtained by a malicious attack used to access data from our customer database. Upon initial review, it	SS
used to access data from our customer database. Upon initial review, it	ound
· ·	er and
appears that some customer data was deleted from the database.	
Protect The team has implemented new authentication policies to prevent futur	
attacks: multi-factor authentication (MFA), login attempts limited to thre	e
tries, and training for all employees on how to protect login credentials.	
Additionally, we will implement a new protective firewall configuration a	nd
invest in an intrusion prevention system (IPS).	
Detect To detect new unauthorized access attacks in the future, the team will u	
firewall logging tool and an intrusion detection system (IDS) to monitor a	

	incoming traffic from the internet.
Respond	The team disabled the intern's network account. We provided training to interns and employees on how to protect login credentials in the future. We informed upper management of this event and they will contact our customers by mail to inform them about the data breach. Management will also need to inform law enforcement and other organizations as required by local laws.
Recover	The team will recover the deleted data by restoring the database from last night's full backup. We have informed staff that any customer information entered or changed this morning would not be recorded on the backup. So, they will need to re-enter that information into the database once it has been restored from last night's backup.