

Access controls worksheet

A payment was made from the organisation to an unknown bank account, the finance manager denied any wrongdoing and claimed they were not aware of the transaction. The business owner has asked me to investigate the event to prevent any similar incidents from happening again.

To understand what happened, I will review the access logs. The access logs will present key information which I will use to identify if there are any threat actors present. Below are my notes, the issues and security recommendations.

	Note(s)	Issue(s)	Recommendation(s)
Authorization /authentication	User: Legal\Administrator IP: 152.207.255.255 Date: 10/03/2023 Computer: Up2-NoGud	Robert Taylor Jr. had access to admin and legal account Since the user is part of the legal team, they shouldn't be able to access payroll resources The user is on a contract which ended on 12-27-2019 however the event log was triggered on 10/03/2023	<i>Role based access control</i> <i>Principle of least privilege</i> <i>Separation of duties</i> <i>User - Deprovision</i>

Event log

Event Type: Information	
Event Source: AdsmEmployeeService	
Event Category: None	
Event ID: 1227	
Date: 10/03/2023	
Time: 8:29:57 AM	
User: Legal\Administrator	
Computer: Up2-NoGud	
IP: 152.207.255.255	
Description:	
Payroll event added. FAUX_BANK	

Employee directory

Lisa Lawrence	Office manager	l.lawrence@erems.net	118.119.20.150	Full-time	▼ Admin	12:27:19 pm (0 minutes ago)	10/1/2019	N/A
Jesse Pena	Graphic designer	j.pena@erems.net	186.125.232.66	Part-time	▼ Admin	4:55:05 pm (1 day ago)	11/16/2020	N/A
Catherine Martin	Sales associate	catherine_M@erems.net	247.168.184.57	Full-time	▼ Admin	12:17:34 am (10 minutes ago)	10/1/2019	N/A
Jyoti Patil	Account manager	j.patil@erems.net	159.250.146.63	Full-time	▼ Admin	10:03:08 am (2 hours ago)	10/1/2019	N/A
Joanne Phelps	Sales associate	j_phelps123@erems.net	249.57.94.27	Seasonal	▼ Admin	1:24:57 pm (2 years ago)	11/16/2020	1/31/2020
Ariel Olson	Owner	a.olson@erems.net	19.7.235.151	Full-time	▼ Admin	12:24:41 pm (4 minutes ago)	8/1/2019	N/A
Robert Taylor Jr.	Legal attorney	rt.jr@erems.net	152.207.255.255	Contractor	▼ Admin	8:29:57 am (5 days ago)	9/4/2019	12/27/2019
Amanda Pearson	Manufacturer	amandap987@erems.net	101.225.113.171	Contractor	▼ Admin	6:24:19 pm (3 months ago)	8/5/2019	N/A
George Harris	Security analyst	georgeharris@erems.net	70.188.129.105	Full-time	▼ Admin	05:05:22 pm (1 day ago)	1/24/2022	N/A
Lei Chu	Marketing	lei.chu@erems.net	53.49.27.117	Part-time	▼ Admin	3:05:00 pm (2 days ago)	11/16/2020	1/31/2020