Shapiro Vladislav

APPROVALS APPROACH DURING PANDEMIC

During this quarantine time, most of us ended up working from too familiar surrounding (a.k.a home) subconsciously not feeling that we are at work. Especially it is true for IT operations people and management, who are not often working off site. This, in combination with irregular working hours due to family and household duties (kids are at home; helpers, like babysitters, cleaners, are not around, etc.) in my opinion, will create a new window of opportunity for suspicious lateral movement and gaining privileged and elevated access rights.

When we are at the office or even working from home regular hours, the request for accessing protected data or any crown jewel application at 11pm would raise the flag and diminish chances of being approved on the spot. But today I can easily imagine the situation when some of us could work only after putting kids to bed, and realizing that they do not have access to something important only that late. Traditional behavioral models based on previous work style would not work and we will be inclined to approve this type of request if the requestor story sounds legit. It definitely creates a window of opportunity for professional “storytellers”, like social engineers. It would be easy to convince an approver at 11pm who is tired of being locked at home and just want to go to bed.

As identity professionals, we need to find the way of helping both: requestor and approver. I would recommend the following: 1) Requestor informs the organization (better via some kind of scheduler tool connected to IAM system) that today he/she is working irregular hours (say from 4pm to midnight) and might need to submit request with very tight deadline. 2) It creates a request in IAM to adjust access request rules. 3) The designated person approves this request, and informs the requestor that he/she can submit access requests during non-regular hours without being flagged. 4) When time comes, requestor submit access entitlement request. 5) Non-regular hours approval workflow starts.

This way, company is ready for possible request, has enough time to assign an emergency/exceptional approver who is expecting the request and knows what to do with it. It will not eliminate the possibility of attack, but at least gives an organization time between steps to verify the identity of the Step 1 requestor and prepare for the probable request event.