All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

MFU – Multifactor Foul Up

Multi-factor authentication has really screwed up a lot of stuff and it's going to get worse and worse until we stop the stupidity.

A simple example

We bought a company. So we wanted to gain control over their financial accounts. Sounds simple enough – you tell the bank(s) with the account(s) about the new ownership, and they switch it over to the new owners who are then in control.

- Were that only true

In our connected world, online access allows us to do stuff online. But actually, that used to be true. Today, it increases the security workload to an unbelievable level. The problem is that each and every account has multi-factor authentication (MFA), and apparently, the only way to change anything about anything means having to do MFA for each activity. And that means that you need control over all of the devices involved everywhere they are involved for every step of the transition, and in many cases multiple times for each step.

- Problem 1: The bank itself sends authentication requests to the phone of the previous owner, who may or may not be available in the 2 minute time frame to complete the authentication.
  - So you end up in long calls or ongoing transactions to get through process.
  - The hardest part of the process is changing phone number for 2FA – which we actually do not want on every account for every person in every situation.
  - For example, read-only access for tax purposes which cannot move any money and is already covered by notification of every action, need not authenticate every time anything is done.
- Problem 2: Group accounts cannot have group 2FA because only one authentication mechanism is allowed (in some cases). But we are not supposed to have group accounts – right? NO!!!
  - We NEED group accounts so that, for example, when a form is filled out on a Web site or when someone is out sick or changes jobs, etc. we can manage who takes over. So accounting, for example, is a business function, not an individual.
  - We use mailing lists for this so the inbound email to the list gets sent to the appropriate people. But if Jane is out sick, John cannot do the multi-factor authentication. So even though John is authorized, because a phone number is used, we cannot complete the process.
  - Unless we have phoney phone numbers taking text messages and also forwarding them to the appropriate phone numbers of the appropriate people who all get the message and end up overlapping each other with different codes for different actions they are taking.

- Problem 3: Each one does it differently.
  - If there was actually a uniform approach, we could possibly rely on something common and manage it. But the reality today is that one after another of the mechanisms works differently, meaning that we need to train and track everything in different ways, all steps manual, because that's the point of MFA – to make sure a person is involved multiple steps in each activity. Which puts sand in the wheels of operating an actual company.
- Problem 4: All of the accounts and services you didn't know about
  - This one is insane. Because there are so many ways you can do things with money, your entity might have 30-50 or more services connected to it that end up moving money in and out of things. Individuals sign up to all sorts of services that end up being used for authentication. Slack channels connected to WhatsApp channels connected to who knows what, each with different authentication steps along the way, all to get the actual MFA details you need to say yes to a simple login, perhaps just to check an email with the 2FA code for the action you were about to take. But wait! It's too late – it expired! So do it again!!!

Cleaning the slate

So we undertook a cleanup, after another few thousand dollars here and there disappeared into account base don automatic payments or similar authorizations we were unaware of till they hit the bank account.

There are two approaches to this; the hard way and the easy way. But which is actually harder and easier you might not be able to figure out.

- **Change banks and accounts:**
  - This sort of helps the issue, eventually. But as it turns out when you close a bank account, you also have to pay anything outstanding, and how do you find out what's outstanding without good records and cooperation? You wait till things bounce or pout in an unlimited supply of cash. Since you cannot do the latter, eventually wither things settle down or you start paying for bounces indefinitely.
  - How do you cancel these subscriptions? Multi-factor authentication. Which you cannot do. Of course there are work-arounds – they usually take a few hours of calling and emailing and providing details you may not have and have to find out. Unless of course there is someone overseas involved in the process in which case you have even more complexity.
- **Try to clean it up item by item:**
  - Of course if you know what the items are, you can do this, and if you have an accountant who can hunt, you can usually get most of them – in a month or three. But then the 1-year periodic payments start to show up… and the auto-renewals… and the emails telling you the cards are bouncing… and and and.
  - Each of these involves more multi-factor authentication processes requiring more work-arounds and delays and so on and so forth.

But that's just the beginning

We have discussed in other articles that the problems with MFA include denial of service attacks and reduced reliability. So during the AT&T outage of however many hours, how do you imagine that MFA worked for all those mechanisms requiring a text message or call to a cell phone in the AT&T system?

Yes, you guessed it – it did not work at all. Which is to say, the interdependencies associated with MFA create availability problems. And they continue to do so. Eventually you will get over it, except of course for hard deadlines and penalties and missed opportunities and and and …

So a one-day accidental outage because of a bad update caused a nationwide outage of MFA capabilities for perhaps 25% of all US operations. Figure that the US GDP at about $365T translates into $1T per day, but AT&T only has about $250B of that per day. So it's only a 1-day outage. And while many of the transactions will be compensated for the next day, it's also all the people and their time consumed, the frustrations, and so forth.

But hey! It's about risk management! So a loss of a few hundred billion in inefficiency from an outage and the day-to-day waste of a minute or so per login has to be traded off against the alternative – right?

How bad was it before?

Here's the thing. I still have accounts with financial institutions that do not use MFA at all. User ID and password over SSL. They may even drop a cookie the first time you use a new computer or browser and send you an email to let you know so you can tell them if it is wrong. And this seems to work well as it has for many years. No change, no hassle, no problem.

The estimated total losses from cyber attacks, only a portion of which MFA can solve came to only about $10B in in 2022, up by 50% from the year before. In 2021, according to the FBI, US losses were about $7B from about 850,000 reported cases. And MFA does not prevent 100% of these. For example, it does nothing against most malware or influence operations, many extortions, information theft, Trojan horses and computer viruses, and on and on.

As of January 2024, there were more than 5 Billion global Internet users. If we assume the value of their time at perhaps $1/hr, and that they take an extra minute to login from MFA per day, and that on average they login only use computers 250 days per year, that's 250 * 5 Billion /60 minutes per hour, that comes to about $20.8B per year in wasted time. Of course our numbers may be a bit off here and there, but I thunk you are starting to get the idea.

From a risk management standpoint, MFA seems to in fact be a loser. What works better? Reasonably UIDs and passwords, independent (perhaps even at times MFA) verification for new platforms accessing an account, and other similar protections running over encrypted channels (i.e., end to end SSL), and perhaps limits on the number of attempts per unit time per account. And did I mention, not allowing people access to password files so they can guess the bloody things!

Conclusions

MFA in the way it is used today is a multifactor foul-up. It is a bad risk management practice as it is being used, it is over-used, and often abused, and I didn't even discuss how it is often bypassed. So get off the MFA bandwagon and start to do some real analysis for sensible solutions.

