Featured in Forbes Tech Council as a response to negative press concerning a security breach

Strengthening Security For The Future: Preparing For 'When'

Strengthening Security for the Future

Preparing for "When"

Businesses are constantly under siege by cyber threats, including credential theft and infostealing. These threats have become increasingly prevalent whether you are an enterprise or a start-up. For those of us operating in the field of identity verification, this has recently translated to continuous implementation of industry-leading best practices.

Leadership Through Credibility in Identity Verification

AU10TIX is dedicated to establishing identity credibility as part of the customer verification process, both online and in person. This is our core mission, or to put it simply – our business relies on it.

Our origins are rooted in airport security, where we developed robust methods to ensure the identity and safety of travelers. This foundational expertise has allowed us to innovate continually, becoming the first to move identity verification to the cloud and to automate the verification process. These advancements have set new industry standards, ensuring the highest levels of accuracy and security.

Our commitment to innovation and security is evident in our approach to handling security challenges. We are devoted to protecting our customers and their identities, making our experience particularly relevant.

Essential Strategies for Navigating Cyber Threats

Facing these challenges requires a multifaceted approach. Here are some strategies that can help safeguard your organization and ultimately protected ours (I'll get to that later):

1. Follow closely any cyber-attacks or incidents that can alert you of current attack trends.
2. Utilize external expertise when needed. Sometimes, a security or forensic expert team can more easily dedicate the required improvements. I found that forming a proactive partnership can accelerate any process when working with external experts.
3. Establish Clear Security Protocols: Well-defined protocols and regular practice simulation and drills ensure the entire organization and all stakeholders are ready to act swiftly and effectively when needed, making the right decision in critical moments.
4. Transparency is the key to instilling trust in your organization and your internal or external team. It also helps any organization deal with rising issues quickly and without hesitation.

Learning and Improving from a Security Challenge

We are all bound to face security challenges. To put it simply, this is the nature of our business. We recently faced a security challenge. In short, eighteen months ago, one of our employees was targeted by an infostealing attempt, which meant somebody accessed his credentials. Although we immediately responded and revised the access to the credentials, we faced a security challenge

eighteen months later. We have been closely studying this incident and have started to implement the lessons we learned rapidly.

The Incident Investigation Became a Learning Opportunity

Our forensic and security teams thoroughly investigated and confirmed that no personal identifiable information (PII) data had been extracted or leaked. This incident underscored the importance of continuous improvement.

Remain Transparent – Always

Throughout the incident, we communicated openly and honestly with our customers and team members. We provided regular updates, demonstrating our commitment to managing the situation responsibly and transparently. This approach not only addressed the immediate issue but also built long-term trust.

Insights and Recommendations on Strengthening Your Security Posture

Here are some key takeaways from our experience that we recommend for any organization:

1. Act Quickly and Decisively: Immediate action can prevent further complications.
2. Conduct Thorough Investigations: Don’t stop at initial fixes; ensure all vulnerabilities are addressed.
3. Embrace Continuous Improvement: Regularly update and harden your security measures and practices, such as gradually rolling out MFA across all your systems.
4. Maintain Vigilance: Continuous monitoring is essential for early threat detection and response.
5. Communicate Clearly: Keeping all stakeholders informed builds trust and helps manage incidents more effectively.

Our Commitment to Security

While challenging, this incident minimally impacted our operations, caused zero damage, and reinforced our commitment to robust security practices. We are dedicated to avoiding potential threats and continuously improving our systems to protect our customers' trust.

To all organizations out there: Learn from our experience. Stay proactive, vigilant, and always prepared to handle the privacy challenges that come your way. Because they will come.