CEO CFO

ceocfointerviews.com
All rights reserved!
Issue: January 19, 2015
The Most Powerful Name in Corporate News

datablink

Advanced Authentication and Transaction Signing Solutions

Shlomi Yanai
President & CEO

CEOCFO: ***Mr. Yanai, what is the idea behind Datablink?***
Mr. Yanai: The idea behind Datablink is to focus on one of the biggest challenges today in the security industry, which is user identity. There is a growing challenge with cyber security and related threats that you hear about in the news every day, such as the recent Home Depot hacking to other attacks. I think the awareness is there. One thing that is common to all those threats is that the involved corporations and financial services face notable troubles surrounding user identities. Today, user identities are one of the main entry points for hackers into our networks and for hackers to steal from accounts and hack financial transactions as they actually take place. At Datablink, the whole idea is to increase dramatically the security of user identities with a new, innovative offering that is unmatched in the marketplace. Datablink aims to be the first security solution that prevents someone from taking over your PC through man-in-the-browser or man-in-the-middle threats. Verifying user operation with transaction signing is key to reducing fraud – and Datablink offers this in a secure, cost-effective solution.

CEOCFO: ***What is your concept and how are you approaching the problem?***
Mr. Yanai: The problem in most of the organizations out there, especially financial institutions, is that to protect their online services, they are using traditional technologies that are 10 years old. They are using one-time passwords and USB tokens. These solutions can be very easily hacked today with basic hacking techniques such as social engineering, and someone taking over your PC (man-in-the-browser). These solutions are simply outdated. One of the most significant problems today involves social engineering, password sharing and protecting the transactions themselves. Our concept is to create the secure channel between the bank or the corporation and our device, which either leverages the mobile device that the user already has, or a physical device that we provide, which is patented.

We establish the secure channel between the bank and the device so that when the user accesses services and identifies himself to the corporation or the portal of the bank, there is always identification that has been established or transaction signing that has been established with a completely secure out of bank channel. Think of it as a completely separate channel between our device and the bank's backend. We use a unique blinking technology where the backend communicates with our device and hackers cannot intercept it. And even if they were able to intercept it, they cannot understand the encrypted blinking channel. We can also communicate with the mobile device, so it completely separates the mobile data channel from the online service data channel. By doing that, it prevents hackers from accessing or stealing credentials while the user is accessing his account. At the same time, we enable users to protect their operations and financial transactions, as many advanced hacking techniques include someone taking over your browser (known as man-in-the-browser).

We enable the user to really see what is happening at the backend of the bank. As an example, let us say a hacker is trying to access my online service. I will receive a notification on my mobile phone that asks if I am trying to access my bank account. The backend will communicate with our device through the secure channel and I would be able to decline it. If I am really accessing my bank account and conducting a transaction, I would receive the notification and be able to approve it and allow the secure access or the transaction to take place. It is the same with our physical device, which offers even greater security because it is a completely independent device that must be present when the user accesses an account or attempts a transaction with the backend of the bank. Additionally, it is designed to prevent any hacker from taking over the device.

CEOCFO: ***What were the challenges in putting the technology together?***
Mr. Yanai: There are two parts. The first one involves the physical device. The challenge is to keep it cost effective. The key for the IP is to create a very secure solution with the blinking technology that will compare in cost with the traditional cheap technologies, like one-time passwords and other related technology. Therefore, when we offer our solution to banks and online services, we enable them to replace existing solutions or upgrade their security level for the same price as their existing solution. Obviously, price is always a sensitive point for corporations and financial services. The other side is the mobile aspect. We had to create a mobile application with a unique offering that supported devices such as the iPhone, iOS and Windows Phone and operates with a single management platform that supports our physical and mobile solution side by side.

CEOCFO: ***Has a similar approach been tried in the past?***
Mr. Yanai: There is no similar advanced authentication and transaction signing solution with similar security capabilities and cost position. Yes, many companies today offer solutions that are mobile-based, so we are not really innovating on the pure mobile app side. However, our innovation is that our mobile app combines data messaging technology and QR code reading technology in one device within the out-of-band channel, enabling QR code readings in the event that data messaging does not work or if you do not have data coverage. We combine the two technologies in one application to create greater usability. There are other mobile-based solutions, but our key differentiator is the fact that we enable the same backend integration for the physical and mobile device. We enable financial services and corporations to pick and choose their method based on the usability and security levels required for each user. We enable organizations to increase the level of the mobile device to physical or vice versa. No one else in the industry mixes the use of the physical device with the unique IP and the significant cost effectiveness that it brings. Datablink is the only security provider to offer this powerful approach to security.

> **"This is something that is truly unique because there are almost no other authentication solutions out there today that are used both to authenticate the user and then to enable the user to sign transactions when they pay a bill or transfer money."**
> **- Shlomi Yanai**

CEOCFO: ***What is the acceptance by the end user of a physical device?***
Mr. Yanai: It is a challenge because people, mainly in the United States, have not accepted the fact that they need to carry a device to identify or authenticate themselves to the bank or to verify and sign transactions when they pay or give money. In other regions, the acceptance is higher, such as in Brazil. We are seeing many more users with physical devices to authenticate themselves to banks and enterprises. In the United States, we mainly see organizations using physical devices because there is higher sensitivity to protect corporate assets. They have employees that work from home or from anywhere, and they want to enable that access anywhere to the backend, and comply with related regulations that mandate those security levels. Therefore, they present a growing demand. The industry is growing quite fast and adopting user authentication. This is why we enabled the combination of a physical device with mobile. Many of our customers will start with the mobile and only a few of the physical, and based on their needs, they will add more or less physical devices.

CEOCFO: ***When you are speaking with a prospective client, is there a aha moment when they really understand the depth or the value of what you are offering or are they skeptical?***
Mr. Yanai: Definitely. I think the key point is that there is a clear awareness in many of the security breaches that we see and many of the customers that already use identification and user authentication solutions are still employing very old security technologies. It is clear that they use one-time passwords or traditional tokens to authenticate users for the corporate network or for their online portal. They can call anybody and share their password, or social engineering can work very effectively for hacking. Anybody can call them claiming they are from the bank or the corporation, find some data on social networks about the user and convince him to provide his one-time password. This is a growing problem for both corporations and financial institutions, and we come with a solution that eliminates that possibility and mandates that either a physical or mobile device be present for the blinking process. Enterprises and many financial services that we target completely get it.

The second piece is that the same device and same solution is used for signing transactions. This is something that is truly unique because there are almost no other authentication solutions out there today that are used both to authenticate the user and then to enable the user to sign transactions when they pay a bill or transfer money. This allows them to make sure of what is signed and prevent common hacking attacks such as someone taking over the PC (man in the browser and man in the middle). Let us say you want to wire $200 from one bank to another. What we enable is that the backend will transfer the full wiring details into the device with the blinking or will push those to the mobile device. The user will see those on the screen, the physical or mobile device, which are external to the PC. They will validate the data, and then the user presses a button and receives a one-time code. The code is encrypted and unique for that specific transaction, so the user can sign the transaction. Hackers cannot know what is going on within the physical device. Therefore, when they hack the session and try to wire those $200 or $100,000 to different accounts, the data that is displayed on the screen will be different, and the user is able to reject the transaction. We are offering both to authenticate users with a very advanced technology that eliminates password sharing or social engineering hacking, and then we also sign the financial transactions themselves with the same device and the same pricing, which is a very unique offering.

CEOCFO: ***Does your personal history in the industry give your potential customers confidence?***
Mr. Yanai: Myself and the rest of the executive team, all of us have a minimum of 10 years of experience in this specific industry. Our CTO is well known in this space, and our leader in strategic sales brings a great deal of experience in this industry. The company itself is not just a startup. The technology was working, implanted, proven, and we support millions of users today in Brazil.

CEOCFO: ***Are you re-launching the company?***
Mr. Yanai: We are re-launching the company as Datablink, so Datablink is using those technologies and completely re-launching itself internationally to leverage the opportunity. If I am a customer, I would want to know it is proven technology with millions of users relying on it successfully. I would want to know if it is easy to use, and we show them how easy it is to use, and you want a cost-effective solution and we show them how you can combine the mobile and physical devices to achieve a very usable and truly cost-effective solution.

CEOCFO: ***What is the strategy for the next year or so? How will you roll out your offering?***
Mr. Yanai: We currently have a very strong presence in Brazil, which we are expanding. The company is completely bootstrapped, and there is no mystery behind the company. Therefore, right now we are investing millions of dollars from the cash that the company generated in advance and the current revenue stream in introducing the new services and solutions I described. The mobile offering is there, and the physical device offering is there. We are extending those with more features and more flexibility, and the strategy is to implement more with what we have as a bootstrapped company that is expanding sales in Latin America and in the United States. We are now in the first stage of expanding into other international markets where we have increased interest. We are now hiring in the United States and Latin America with a significant focus in technical services and development.

CEOCFO: ***Do you feel you are still a little bit ahead of your time? Is even the U.S. ready?***
Mr. Yanai: I think that corporate banking is ready. When I think about the financial services market, there is corporate banking, which is definitely ready, and there are many solutions that are already implemented. Private banking is definitely ready, and people make transactions of hundreds of thousands of dollars, so they have the awareness and willingness to carry the device or use the mobile solution. Even retail banking on some level is ready. The recent incidents in the United States make people more aware of the risks. Regarding your earlier question about people being willing to carry a physical device, I think that if they knew that this is secure and would minimize the risk, they would do so. There are 7,000 financial institutions in the United States, but we are not just targeting the first tier. We are also targeting the second tier, the regional banks and the different financial institutions. For them, we can be a great solution, as well as for the large corporations that are still running on solutions that were implemented years ago, which are password-based and no longer secure. We can offer them a very clear replacement alternative.

Interview conducted by: Lynn Fosse, Senior Editor, CEOCFO Magazine

Datablink Inc.

For more information visit:
www.datablink.com

Contact:
Sandra Magnani
703-639-0600
sandra@datablink.com