CARLTON FIELDS

The Missing Piece: Engaging Employees in Building Zero-Trust Environments

November 01, 2021

With the recent proliferation of “zero-trust” environments in enterprise security, there has been an implementation bias toward technological solutions to secure data and prevent unauthorized access to systems. When the approach is driven by IT and other technical teams inside an enterprise, it should be no surprise that this would be the case. This is not a criticism but rather a reflection of domain expertise. Businesses should rely on their resident experts to implement the technical infrastructure necessary to protect business assets and personal data.

Due to the fact that employees and teams have been working in a distributed fashion throughout the COVID-19 pandemic, employing technological solutions that can be remotely deployed is also an efficient means to arrive at a zero-trust security environment.

As a result of the new work-from-home paradigm, many businesses rushed toward multifactor authentication and other forms of identity access management. Yet, the state of enterprise security is still, in large part, subject to human error. Once employees verify their legitimate access to business systems, they begin to operate from the knowledge basis of how they were trained and supported to understand security risks.

In moving toward zero-trust environments, businesses must turn their focus to “security by design” principles and, specifically, by revisiting the oft-forgotten principle of “psychological acceptability.” This principle, at its core, focuses on (1) the avoidance of security measures being seen as obstructions to users which they are intent to work around and (2) methods to encourage or invite users to embrace given security measures.

Zero Trust Still Needs a Human Touch

The missing piece in most enterprise security programs is the support of employees and real training. To assume that mandatory security training is going to cut it for most employees is a dangerous assumption.

It is not about training the right team. It is not even about training members of all teams on how to identify security threats.

Employees must be meaningfully engaged in the protection of business assets and systems and understand this to be a part of their job functions. Information made available to employees, their training, and ongoing support must be tailored to specific roles and job functions.

Policies must be developed in a manner that appreciates the existing roles and responsibilities of each employee. When a training or tabletop security exercise is added to existing job functions, it is viewed as an extra burden. When training and support are built into job roles and functions, it is clear to employees that security, and ethics in data management and governance, are part of the corporate ethos. The business is demonstrating a commitment to its security practices.

Communication is an important part of implementing meaningful security measures. Different employees come to the table with different skill sets and experience with privacy and security. If it is not communicated to employees how security measures apply to them and their distinct job roles, it's as if two individuals are talking past one another. The teams responsible for security are speaking a technical language and advocating for the architecture and solutions that they had the decision-making authority to choose; the other employees are forced to accept this architecture and solutions without a true understanding of why they are important.

Employees have to be empowered to report security risks. Technological solutions cannot be communicated to employees as the be-all, end-all. For example, if the implementation of multifactor authentication is the direct result of an unauthorized access incident, and it is communicated that the multifactor authentication is the solution to the problem, this approach may overlook the "human mistake" factors that could still lead to future incidents involving unauthorized access or other security breaches. These technological solutions do not necessarily address the litany of other ways businesses find themselves facing a security breach.

People and systems, not just systems, are ultimately responsible for successful security programs.

Zero Trust Should Not Erode Trust with Employees

Beyond some of the obvious technology implementations that allow businesses to verify the identities of the individuals logging into their systems, many companies have implemented various forms of remote monitoring technologies to monitor employees' work and performance throughout

the day. While the prevalence of these technologies may be suited better to some industries than to others, they must be implemented with care and respect to U.S. state laws and the laws of other jurisdictions in which a business may operate. Businesses should ensure that they have a legitimate, legal basis for implementation. A business should be ready to engage in an open dialogue with its employees, about why the implementation is necessary. Further, in some U.S. states and other jurisdictions, consent must be obtained for the implementation of such monitoring technologies.

Business decisions around security must factor in the principle of psychological acceptability. These technologies should also be evaluated for their reception in your particular business environment as that will lead to whether such technologies will be efficacious. If employees are made to believe they are part of the problem (i.e., they did something wrong that has led to the implementation of these technologies and that their personal autonomy and space is being intruded upon as a result), they are less likely to be engaged in the security of the company and the data of which the company is a steward.

The "Why" for Enterprise Security

The larger question regarding truly institutionalizing an ethos with employees around security is determining the driving force behind security programs. The unfortunate reality is that many businesses continue to place policy and technical Band- Aids on security problems rather than approaching security from a "security by design" perspective. Security is not infused into every company process. Rather, it is applied on an ad hoc basis when deemed necessary, which is often driven by an outside force. The rapid acceleration of zero trust throughout the COVID-19 pandemic was driven by the pandemic and the need to quickly get organizations of all sizes operating remotely, at as close to the same capacity as they were operating pre-pandemic. It is hard to know if this acceleration would have occurred without the necessity for it.

There are other "why" factors for the implementation of security measures, and businesses should take care to evaluate whether the right factors are the ones propelling the development of their security policies, programs, and systems.

Customer Demands

If customers (not users) are driving the need for enhanced enterprise security measures, through contractual demands placed on a business or organization to assist in business development and customer acquisition, these measures may be specific to the customer versus purposefully being built into the policies, programs, and systems of the business. Having different customers with different rules of the road for each use case results in a patchwork of security approaches that effectively become a customer appeasement strategy versus a comprehensive security program.

Regulation

If regulation serves as the driving force behind the implementation of new security measures, there is a tendency for businesses to see the regulations as a "floor" instead of reaching for the "ceiling." Many businesses evaluate regulations for what is precisely required to comply with a specific regulation. When the implementation of enterprise security measures flows from an obligation versus an aspiration to protect the business's customers and employees, the security program will likely miss the mark.

Users and Data Stewardship

If protecting users and data stewardship is the driving force for adopting "best of breed" security, this requires an intentional design of privacy and security programs in such a manner that privacy and security are embedded in every policy, program, and system of the business. This is a much more involved approach but, in the long term, is the approach most likely to avoid costly security issues that may emerge.

Balancing the Elimination of User Error and User Buy-In

Zero trust is about eliminating user error. The benefits of this elimination of opportunity for users in systems to cause massive exposure to a business are clear; but regardless of the technology advancements, businesses are still driven by the people who manage them and work for them. The absence of supports for employees in this new paradigm may create scenarios in which reliance on systems that seemingly eliminate the need for voluntary employee security measures may, as an unintended consequence, create new security risks.

This article was first published in CISO MAG, an EC-Council publication.

Related Practices

Cybersecurity and Privacy

accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.