Best Security Practices to Prevent Insider Breaches and Protect Systems

Information security has become a critical priority for IT Support teams, especially in an environment where both internal and external threats increase every year. According to the *Verizon Data Breach Investigations Report (DBIR 2023),* 74% of security breaches involve a human element, underscoring the importance of strengthening daily operational practices. At **NetGuard Solutions**, we have observed that many vulnerabilities originate from misconfigurations, excessive privileges, and a lack of continuous monitoring.

One of the most essential best practices is implementing the principle of least privilege, recommended by CISA, which limits potential damage if an account is compromised. Complementing this is the need for multifactor authentication (MFA), especially for remote access and administrative panels. Another critical measure is maintaining strict patch management, as IBM Security's *Cost of a Data Breach Report 2023* indicates that breaches caused by unpatched vulnerabilities cost organizations an average of 33% more.

For support engineers, it is crucial to combine these practices with constant monitoring of network traffic. Tools like ***NetGuard Pro*** help detect anomalies, automate responses, and ensure operational continuity even in complex environments. Finally, promoting an internal culture of security through brief, periodic training sessions helps reduce human errors and strengthen organizational resilience.

By applying these practices, support teams can better protect critical systems, minimize risks, and ensure that their organization's technological infrastructure is ready to face modern threats.

Mejores Prácticas de Seguridad para prevenir brechas internas y proteger sistemas.

La seguridad de la información se ha convertido en una prioridad crítica para los equipos de Soporte de TI, especialmente en un entorno donde las amenazas internas y externas aumentan cada año. De acuerdo con el *Verizon Data Breach Investigations Report (DBIR 2023)*, el 74% de las brechas de seguridad involucran un elemento humano, lo que subraya la importancia de fortalecer prácticas operativas diarias. En **NetGuard Solutions**, hemos observado que muchas vulnerabilidades se originan en configuraciones incorrectas, privilegios excesivos y falta de monitoreo continuo.

Una de las mejores prácticas fundamentales es la implementación del principio de privilegios mínimos, recomendado por CISA, que limita el daño potencial si una cuenta es comprometida. A esto se suma la necesidad de autenticación multifactor (MFA), especialmente en accesos remotos y paneles administrativos. Otra medida crítica es mantener una gestión estricta de parches, ya que según IBM Security (Cost of a Data Breach Report 2023), las brechas causadas por vulnerabilidades no parcheadas cuestan en promedio un 33% más a las organizaciones.

Para ingenieros de soporte, es clave combinar estas prácticas con un monitoreo constante del tráfico de red. Herramientas como ***NetGuard Pro*** permiten detectar anomalías, automatizar respuestas y asegurar la continuidad operativa, incluso en entornos complejos. Finalmente, promover una cultura interna de seguridad mediante capacitaciones breves y periódicas ayuda a reducir errores humanos y fortalecer la resiliencia organizacional.

Al aplicar estas prácticas, los equipos de soporte pueden proteger mejores sistemas críticos, minimizar riesgos y garantizar que la infraestructura tecnológica de su organización esté lista para enfrentar las amenazas modernas.