PASOS PARA MEJORAR LA CIBERSEGURIDAD

PREPARAR

Las empresas deben prepararse para los ciberataques. Los tres primeros pasos para prepararse para un ciberataque en su negocio implican PERSONAS, SISTEMAS y BACK-UPS.
Primer paso: SISTEMAS, defina procesos orientados a la seguridad basados en estándares como ISO27001, ISO 27032, NIST CSF, mejor aún si lo implementa.
Segundo paso: Las PERSONAS, se debe educar a los empleados sobre la amenaza, empezando por el uso de contraseñas seguras y el aprendizaje sobre amenazas como el phishing.
Tercer Paso: Buen sistema de Backup, en caso de ataque, le permite empezar de nuevo.

DETECTAR

Debe tener un equipo propio atento a lo que sucede en su equipos de seguridad o contratar una empresa especializada como PROJECTNET. Soluciones de visibilidad como un SIEM o un Orquestador de Seguridad apoyan en la gestión y visibilidad de nuestra solución. Manténganse al día de las noticas de seguridad sobre las amenazas emergentes y las actualizaciones de seguridad. Practique la seguridad ofensiva, y pase por un Ethical Hacking o tenga un analizador de vulnerabilidades en su red.

RECUPERAR

Después de responder adecuadamente al incidente, ahora se debe recuperar el sistema y dejarlo tal y como estaba antes del incidente. Para ello se deben implementar medidas de recuperación de la información como tener listos los backups, copias de seguridad. Tener planes de continuidad de negocio, que incluyan incluso borrado de información en caso de robo.

PREVENIR

Algunos appliances que las Empresas pueden emplear para ciberseguridad son: firewalls, IPS, EDR, autenticación por doble factor, NAC, AntiDDoS, Proxy, política de paswords, políticas de seguridad. Las aplicaciones también deben ser seguras o ponerle un WAF para mayor seguridad.

RESPONDER

Cuando se detecta un incidente, es importante responder a conciencia y a tiempo. Trabajar con su proveedor de seguridad (PROJECTNET) para contener, mitigar y eliminar la amenaza.
Se debe alertar a las partes afectadas y proporcionarles informes de progreso a lo largo del incidente. Asegurarse de que todos los elementos del atacante son eliminados de los sistemas afectados, determinar la causa y los síntomas del incidente, parchar todas las vulnerabilidades y restaurar los datos adecuadamente a partir de las copias de seguridad.

PROJECTNET

info@projectnet.com.pe

SOLUCIONES PARA LA CIBERSEGURIDAD

PREPARAR

Servicio de Oficial de seguridad como servicio

Respaldo: VEEAM datto PROJECTNET

DETECTAR

Análisis de vulnerabilidades: tenable

SIEM: RSA

PROJECTNET

PREVENIR

Protección del EndPoint: SentinelOne kaspersky eset SOPHOS

Firewall UTM: FORTINET Check Point JUNIPER NETWORKS CISCO

Correo seguro: Barracuda FORTINET CISCO

Proxy: CISCO Barracuda FORTINET

Autenticación por doble factor: RSA OneSpan

NAC: aruba CISCO FORTINET

WAF: radware Barracuda

Anti DDoS: radware

DNS Seguro: CISCO Infoblox

CASB: FORTINET Check Point

Firma Digital: OneSpan Validated ID

Criptografía (HSM/PKI/CA) : utimaco realsec

PROJECTNET

RESPONDER

PROJECTNET

RECUPERAR

Respaldo: VEEAM datto

PROJECTNET

PROJECTNET

info@projectnet.com.pe