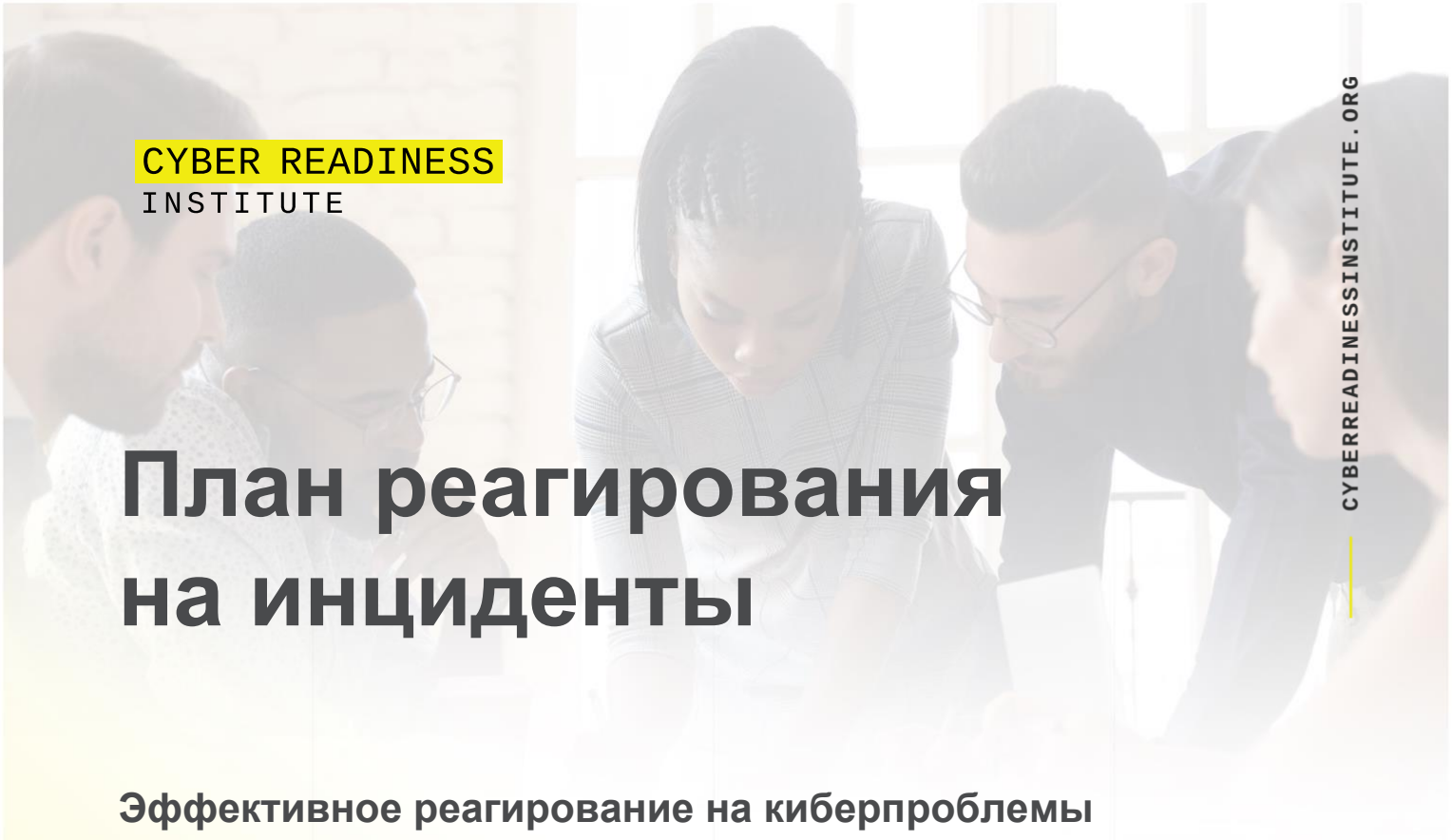

CYBER READINESS
INSTITUTE

CYBERREADINESSINSTITUTE.ORG

План реагирования на инциденты

Эффективное реагирование на киберпроблемы

Установление практики и политики киберготовности помогает снизить риск, но важно исходить из того, что нашей компании, вероятно, в какой-то момент придется столкнуться с инцидентом безопасности, который может повлиять на бизнес-операции. Пытаться определить, как реагировать во время инцидента, - не очень хорошая идея. Время реагирования имеет решающее значение для минимизации ущерба. Наличие четкого плана может предотвратить катастрофу в результате инцидента.

Обзор

Комплексный пошаговый план реагирования на инциденты позволяет нам быстро реагировать на инциденты, разрешать их и извлекать уроки из каждого инцидента. Этот план реагирования на инциденты служит дорожной картой того, что делать при реагировании на инцидент безопасности, и является гарантией того, что у нас имеется стратегический, а не реактивный ответ.

Реагирование на инциденты состоит из трех основных элементов:

1. **Подготовка** к возможному инциденту в будущем
2. **Реагирование** во время инцидента
3. **Восстановление** после инцидента

Как подготовиться

Организационные принципы:
Как и во многих других вещах, небольшая подготовка имеет большое значение. Есть несколько основных действий, которые необходимо выполнить как можно скорее, чтобы должным образом подготовиться к атаке и уменьшить ущерб от нее.

1. **Сделайте резервную копию данных и убедитесь, что вы можете восстановить данные из резервных копий.** Восстановление после атаки пройдет намного быстрее и повлияет на работу гораздо меньше, если у вас есть текущие резервные копии системного программного обеспечения, приложений и особенно важных данных. Вы также должны убедиться, что у каждого сотрудника в вашей организации есть резервные копии, если вы не делаете это централизованно. Необходимо регулярно тестировать резервные копии.
    - ✓ Дата копирования: [ДАТА]
2. **Убедитесь, что все знают, как сообщить о возможном инциденте.** Раннее выявление действительно важно. Каждый член команды должен знать то, как обнаружить подозрительную активность и к кому обратиться по этому поводу.
    - ✓ Назначенное контактное лицо компании: [КОНТАКТНЫЕ ДАННЫЕ]
    - ✓ Дата выполнения: [ДАТА]
3. **Найдите хорошую техническую внешнюю поддержку по реагированию на инциденты.** Знайте, к кому идти и как связаться со службой внешней поддержки в чрезвычайной ситуации. Пожар, который вы не в состоянии контролировать, требует вызова пожарных. Вам нужно знать, кому звонить, если вы не можете контролировать киберинцидент. Как минимум, это должен быть эксперт по ИТ-поддержке, которого вы знаете и которому доверяете. В зависимости от масштаба и характера вашего бизнеса целесообразно определить дополнительные средства связи и юридическую поддержку.
    - ✓ Назначенное контактное лицо службы внешней поддержки: [КОНТАКТНЫЕ ДАННЫЕ]
    - ✓ Дата выполнения: [ДАТА]

Как реагировать

На компьютере сотрудника происходит что-то безумное, и он не знает, что делать. Это то же самое, что почувствовать запах дыма или увидеть небольшое пламя в кофейне.

Вот что нужно сделать:

1. **Изолируйте проблему:** немедленно отключите устройство от сети
2. **Определите вид инцидента** и выполните следующие действия:

   - ✓ Вредоносное ПО – немедленно отключите устройство от сети
   - ✓ Кража учетных данных – заблокируйте, но не удаляйте аккаунт, сбросьте пароль
   - ✓ Утечка данных – позвоните в экстренный отдел ИТ
   - ✓ Программы-вымогатели – немедленно отключите устройство от сети
   - ✓ Отказ в обслуживании – свяжитесь с вашим менеджером/ИТ-специалистом/интернет-провайдером

3. **Определите масштаб** инцидента, задав эти вопросы:

   - ✓ Когда произошел инцидент?
   - ✓ Кто пострадал?
   - ✓ Какова техническая природа инцидента? Как это произошло?
   - ✓ Кто знает об инциденте?
   - ✓ Он все еще продолжается?

4. **Определите, можно ли должным образом контролировать его внутренними усилиями компании,** или нужно ли вам позвонить во внешнюю службу ИТ-поддержки чтобы убедиться, что вы справились со взломом надлежащим образом.
5. **Продолжайте проверять, не повторится ли проблема.** Если неясно, решена ли проблема, проявите осторожность и обратитесь к специалисту по поводу проблемы.

Как восстановить

Кризис миновал, пора возвращаться к нормальной жизни. Масштаб инцидента и серьезность воздействия будут определять то, сколько времени и усилий потребуется для восстановления. Тем не менее, основные шаги одинаковы.

Вот что вы должны сделать:

1. Уведомите все пострадавшие стороны
2. Смените идентификатор пользователя и пароль скомпрометированного устройства
3. Исправьте все устройства
4. При необходимости переустановите программное обеспечение и данные из резервных копий

Dhgljhevguc kibkhd j_Z]bjh\Zgby gZ bgpb^_glu

Wlhl dhgljhevguc kibkhd ^he`_g ihfhqv Bldbf[_gj_^`yjm куратору beb

Ih^]hlh\a

P_a_j\gh_ dhibjh\Zgb_ ежедневно

9 GZkljhcdZ **подтверждение** Z\lhfZlbq_kdh]h j_a_j\gh]h dhibjh\Zgby: [>**ATA**]

L_klh\u_ j_a_j\gu_ dhibb dZ`^u_ ljb f_kypZ

9 >ZlZ ihke_^g_]h **копирования**: [>**ATA**]

Обучение персонала протоколу регистрации личности (IRP)

9 >ZlZ ihke_^g_]h **обучения**: [>**ATA**]

DhglZdlgh_ ebph ^ey wdklj_gghc поддержки \b BB BBBBBBBBBBBBBBBBBBBBBBBBBBBBB
Bgl_jg_l ijh\Zc^_j BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
DhglZdlgh_ ebph ^ey wdklj по юридическим вопросам BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
DhglZdlgh_ ebph ^ey wdklj_gghc k\yab BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB

J_Z]bjh\Zние

Bahebjmcl_ ijh[e_fm ² hldexqbl_ mkljhckl\h hl k_lb

Hij_^_eb\ид bgpb^_glZ

† DjZ`Z mq_lguo ^Zgguo

† Ijh]jZffu \ufh]Zl_eb

† <j_^hghkgh_ IH

† HldZa \ h[kem`b\Zgbb

† Ihl_jy dhgnb^_gpbZevguo ^Zgguo

Hij_^_ebl fZkrlZ[bgpb^_glZ

† Dlh ihkljZ^Ze"

† Dh]^Z wlh gZqZehkv"

† Wlh \k_ _ijh^олжается"

<hkklZgh\ление

M_^hfbl_ \k_ klhjhgu

Смените b^_glbnbdZlhj ihevahiZl_ey b \Zjb_eyk dh fijhf_lbjh\Zggh]h mkljhckl\Z

Установите исправности на \k_ mkljhckl\Z

Ijb g_h[oh^bfhklb i_j_mklZgh\bl_ h[_ki_q_gb_ b ^Zggu_ ba j_a_j\guo dhibc

>hihegbl_evgu_ j_dhf_g^Zpbb ih j_Z]bjh\Zgbx gZ bgpb
Wlh jmdh\h^kl\h ^he`gh ihfhqv BL f_g_^`_jy to b db[_j

?keb \u hlb, чтобы в вашей организации был [he__ gZ^_`guc ieZg j_Z]bjh\Zgbx^b yg guZ`_
ijb_^_g q_luj_owlZiguc ih^oh^ hkgh\Zgguc gZ j_dhf_g^Zpbyo GZpbhgZevgh]h bgklbl
l_oghehgbl. Однако 1,67 Вероятно, вы не сможете ke_^h\Zlv dZ`^hfm rZ]m gh k^_eZcl_ \k_ \hafh`gh_
qlh[u ^_ckl\h\Zlv gZ dZ`^hf ba q_luj_o rZ]h\ lZdbf h[jZahf qlh[u wlh bf_eh kfuke ^ey
hj]ZgbaZpbb

1 Ih^]hlh\dZ

Ih^]hlh\dZ y\ey_lky dexqhf d [ukljhfm j_Z]bjh\Zgbx
GZ wlhf wZpe \u khklZ\ey_l_ kibkhd \k_o \Zrbo ZdlbZh\
² Ih]h что позволяет вашей компании в сети свою
деятельность Wlhl kibkhd [m^_l \dexqZlv ihfbfh
ijhq_]h k_j_ju k_lb ijbeh`_gby b djblbq_kdb
\Z`gu_ dhg_qgu_ lhqdb gZijbf_j ghml[mdb Ihlhe_d\mh^Z
lh]h dZd \u khklZ\beb kibkhd ihdZ\ZZ\ZZ\ZZ
bo ih kl_i_gb \Z`ghklb bkeZ\e_fbo fh^_eb
ljZnbdZ qlh[u \u fh]eb kha^Zlv [Zah\u_ ihdZaZl_keb
dhlhju_ [m^ml bkihevah\Zlvky ^ey kjZ\g_gby ihaZ_kijhkbjZgbeZk\ymgZa^_kv m \Zk [m^_l
gZcfbl_ ihklZ\ydmZ^ey fhgblhjbg]Z bo fh^_e_c [hevr_ jZ[hlu
ljZnbdZ _\kmbo жете выделить на это средства.
?keb \u g_ fh`_l_ iha\heblv k_[_ycmrkgZ\sbdZ
начальном этапе [m^mправильно составить kibkhd
Zdlb\hlyудалить ijbhjbl_lgh_ \gbfZgb_ d \Zrbf
Zdlb\Zf Kha^Zcl_ieZg действия k
j_dhf_g^Zpbyfb h lhf k d_f k\yaZlvky dZd b dh]^Z ^ey
dZ`^hfjZa bgpb^_glZ G_ aZ[m^vl_ k\yaZlvky kh
\k_fb ba wlh]h kibkdZ ^h lh]h dZd \hagh djbabk
H[uqguc j_nj_g \ Zglbdjbabkghf mijZ\e_g ©<u
gbdh]^Z g_ ^he`gu h[f_gb\Zlvky \bablgufb ljlhqdZfb
\h \j_fy djbabkZª M[_^bl_kv qlh \k_ \ \Zr_f kibkhl rZ] ^Z_l \hafh`ghklv ba\e_qv mjhdb ba
agZxl q_]h \u h`b^Z_l_ hl ghuидентаj_fy \Zr_]h hiulZ qlh[u \u fh]eb emqr_
j_Z]bjh\Zlv gZ [mhидеты
[_ahiZkghklb Как бы ни было велико искушение
Hij_^_ebl_ dZdb_ kh[ulby [_ahiZkghklb b ijb dZdbhmklblwlhl rZ] hkh[_ggh k \Zrbf
ihjh]h\uo agZq_gbyo [m^ml aiZeZgkjZZ\b\Zr [_kdhg_qguf kibkdhf ^_e gZklhyl_evgh
jh\Zgby gZ bgpb^_glu Qlh[u ihfhqv \Zf hij_^_eblv dhf_g^m выполнить его.
ihjh]h\u_ agZq_gby ih^mfZcl_ h lhf qlh fh`_l
gZjmrblv \Zrb [bag_k hlkZ_bhij_^_e_gby
wlbo ihjh]h\uo agZq_gbc kha^Zcl_ ieZg j_Z]bjh\Zgby
gZ bgpb^_glu ^ey dZ`^hgjhb^_glh\ ?]h fh`gh
memqrklv ihfhsvпромежуточных требований \h
\j_fy dhlhjuобудете \uy\ey ijh[_eu \k\h
ijhp_kk gh _]h lZd`_ fh`gh memqrblv ihke_
j_Zevguo kh[ulbc ih^jh[g__ h[wlhf iha`_ Kmlv\
lhf qlh[u gZeZ^blv ijhp_kk

2 H[gZjm`_gb_ b ZgZeba

GZ wlhf wlZi_ ijhp_kkZ [ue \uy\e_g bgpb^_gl
[_ahiZkghklb A^_kv \u i_j_oh^bl_ \ j_`bf
bkke_^h\Zgby Kh[_jbl_ \k_ qlh kfh`_l_ h[
bgpb^_gl_ AZl_f ijhZgZebabjmcl_ ^Zggu_
Hij_^_ebl_ lhqdm \oh^Z b rbjbgm [j_rb Wlhl
ijhp_kk agZqbl_evgh mijhsZ_lky b mkdhjy_lky
keb \k \Zrb bgkljmf_glu [_ahiZkghklb
nbevljmxlky \ h^ghf f_kl_ <hafh`gh \u
gZgyeb ihklZ\ydmZdhlhjuc fh`_l
\uihegylv wlb nmgdpbb aZ \Zk

3 K^_j`b\Zgb_ ликвидация b \hkklZgh\e_gb_

K^_j`b\Zgb gZijZ\eo_gZ hklZgh\dm
«djh\hl_q»gbkv \u bkijZ\ey_l_
_keb m]jhaZ ijhgbdeZ ba h^ghc kbkl_fu b
jZ_kijhkbjZgbeZk\ymgZa^_kv m \Zk [m^_l
[hevr_ jZ[hlu

<hkklZgh\e_gb_ направлено на приведение
kbkl_f \ jZ[hq__ khklhygb_ _keb hgZ \ureZ
ba kljhy beb ijhklh _jgmlvky d h[uqghfm
j_`bfmjZ[hlu _keb wlh g_ lZd

4 Извлеченные уроки

Wlh \Zr_]h hiulZ qlh[u \u fh]eb emqr_
j_Z]bjh\Zlv gZ [mhидеты
[_ahiZkghklb Как бы ни было велико искушение
Zdlbhmklblwlhl rZ] hkh[_ggh k \Zrbf
[_kdhg_qguf kibkdhf ^_e gZklhyl_evgh
]_dhf_g^m выполнить его.

<a]eygbl_ gZ bgpb^_gl kdjhfguf gh
dZ`dbq_kdbf \a]ey^hf qlh[u hij_^_eblv
h[eZklb ^ey memqr_gby AZl_f ^h[Z\vl_ wlb
memqr_gby \ k\hx ^hdmf_glZpbx

Gb h^bg ijhp_kk g_ b^_Ze_g ^ey \k_o
\hafh`guo kp_gZjb_\ G_dhlhju_ kp_gZjbb
g_evay ^Z`_ ihgylv ihdZ\ZZ\ZZ\ZZ
EZg^rZnl m]jha lZd`_ ihklhyggh jZa\b\Z_lky
ihwlhfm \Zr ijhp_kk j_Z]bjh\Zgby gZ
bgpb^_glu _kl_kl_ggh [m^_l \j_fy hl
\j_f_gb h[gh\eylvky Надеемся, вы сами
себе скажите спасибо. DZ]h\hjblkhe ©
упустите хороший кризис».